

(19) 世界知的所有權機關
國際事務局



(43) 國際公開日
2001 年 1 月 11 日 (11.01.2001)

PCT

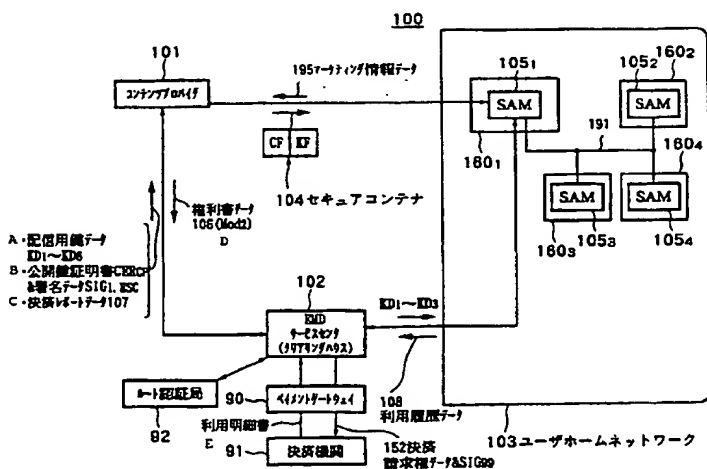
(10) 国際公開番号
WO 01/02968 A1

- | | | | |
|----------------|--|---|----|
| (51) 国際特許分類: | G06F 15/00, 17/60, H04L 9/08, 9/32, G10K 15/02, G06F 13/00 | 特願2000/126305 ✓ 2000年4月21日 (21.04.2000) | JP |
| (21) 国際出願番号: | PCT/JP00/04488 | (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP). | |
| (22) 国際出願日: | 2000年7月6日 (06.07.2000) | (72) 発明者; および | |
| (25) 国際出願の言語: | 日本語 | (75) 発明者/出願人 (米国についてのみ): 野中 聡 (NON-
AKA, Akira) [JP/JP]. 江崎 正 (EZAKI, Tadashi) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). | |
| (26) 国際公開の言語: | 日本語 | | |
| (30) 優先権データ: | | (74) 代理人: 佐藤隆久 (SATO, Takahisa); 〒111-0052 東京都台東区柳橋2丁目4番2号 宮木ビル4階 創進国際特許事務所 Tokyo (JP). | |
| 特願平11/192413 ✓ | 1999年7月6日 (06.07.1999) | JP | |
| 特願平11/193561 ✓ | 1999年7月7日 (07.07.1999) | JP | |
| 特願平11/193562 | 1999年7月7日 (07.07.1999) | JP | |

〔続葉有〕

(54) Title: DATA PROVIDING SYSTEM, DEVICE, AND METHOD

(54) 発明の名称: データ提供システム、装置およびその方法



(57) Abstract: A content provider (101) distributes a secure container (104) containing content data encrypted with a content key data, content key data encrypted with distribution key data, and title deed data encrypted and representing the handling of the content data to, e.g., an SAM (105_i) of a user home network (103). The SAM (105_i) decodes the content key data and title deed data contained in the secure container (104), and determines the handling including the form of purchase and the form of the use of the content data according to the decrypted title deed data.

```

A...DISTRIBUTION KEY DATA KD1 TO KD6
B...PUBLIC KEY CERTIFICATION CERE1 & SIGNATURE DATA SIG1, ESC
C...SETTLEMENT REPORT DATA 107
101...CONTENT PROVIDER
D...TITLE DEED DATA 106(Mod2)
195...MARKETING INFORMATION DATA
104...SECURE CONTAINER
92...ROUTE AUTHENTICATION AGENCY
102...END SERVICE CENTER (CLEARING HOUSE)
90...PAYMENT GATEWAY
E...USE SPECIFICATIONS
91...SETTLEMENT INSTITUTION
108...USE HISTORY DATA
152...SETTLEMENT CLAIM DATA & SIG99
103...USER HOME NETWORK

```

〔続葉有〕

WO 01/02968 A1



(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書
- 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

(57) 要約:

コンテンツプロバイダ101は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ104をユーザホームネットワーク103のSAM105、などに配給する。SAM105、などは、セキュアコンテナ104に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

明細書

データ提供システム、装置およびその方法

技術分野

本発明は、コンテンツデータを提供するデータ提供システム、データ提供装置およびそれらの方法と、これらに用いられる管理装置およびデータ処理装置に関する。

背景技術

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のEMD (Electronic Music Distribution: 電子音楽配信) システムがある。

図100は、従来のEMDシステム700の構成図である。

図100に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a, 705b, 705cには、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵デー

タを用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納したセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA(Conditional Access)モジュール711に送信する。

CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。

この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益分配を行う。

このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益分配は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

ところで、SCMSは、CD (Compact Disc) からDAT (Digital Audio Tape) への録音を防止するために規定されたものであり、DATとDATとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダを特定するに止まり、違法なコピーを技術的に阻止するものではない。

従って、上述した図100に示すEMDシステム700では、コンテンツプロ

バイダの権利（利益）が十分に保護されないという問題がある。

また、上述したE M Dシステム700では、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

また、上述したE M Dシステム700では、ユーザの端末装置709からの課金情報721を、サービスプロバイダ710の権利処理モジュール720で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうか懸念される。

発明の開示

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンツプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置と管理装置とを提供することを目的とする。

また、本発明は、コンテンツプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置と管理装置とを提供することを目的とする。

上述した従来技術の問題点を解決し、上述した目的を達成するために、第1の発明のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書

データとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

第1の発明のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

また、第1の発明のデータ提供システムは、好ましくは、前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する。

また、第1の発明のデータ提供システムは、好ましくは、前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置をさらに有する。

また、第2の発明のデータ処理装置は、データ提供装置から配給されたコンテンツデータを利用するデータ処理装置であって、コンテンツ鍵データを用いて暗

号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第3の発明のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

第3の発明のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが配給される。

次に、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定され

る。

また、第3の発明のデータ提供システムは、好ましくは、前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する。

また、第4の発明のデータ提供システムは、データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記複数のデータ配給装置に提供し、前記第1のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、前記第2のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第5の発明のデータ提供システムは、少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムであって、前記第1のデータ提供装置は、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、第2のコンテンツ鍵データを用いて

暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する。

また、第6の発明のデータ提供装置は、コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する。

また、第7の発明のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コン

テンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第 8 の発明のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第 9 の発明のデータ提供方法は、データ提供装置と、少なくとも第 1 のデータ配給装置および第 2 のデータ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを提供し、前記第 1 のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを配給し、前記第 2 のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 3 のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第 2 のモジュールおよび前記第 3 のモジュールに格納された前記コンテンツ鍵データお

よび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

また、第10の発明のデータ提供方法は、少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記第1のデータ提供装置から前記データ配給装置に、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを提供し、前記第2のデータ提供装置から前記データ配給装置に、第2のコンテンツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する。

また、第11の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は

、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

このとき、前記管理装置による前記権利書データの正当性の証明は、例えば、権利書データに対しての前記管理装置の署名データを作成することによって行われる。

第 11 の発明のデータ提供システムでは、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

また、第 11 の発明のデータ提供システムは、好ましくは、前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

また、第 11 の発明のデータ提供システムは、好ましくは、前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う。

また、第 11 の発明のデータ提供システムは、好ましくは、前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う。

また、第 12 の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

第 12 の発明のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給する。

次に、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

また、第13の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

第13の発明のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給する。

次に、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用する。

また、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

第14の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、前記データ配給装置は、前記提供されたコン

コンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

第14の発明のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供する。

次に、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給する。

次に、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行う。

また、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

また、第15の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

また、第16の発明の管理装置は、コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該コンテンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータを前記コンテンツ鍵データを用いて復号した後に当該コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であっ

て、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する。

また、第 17 の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する。

また、第 18 の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する。

また、第 19 の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給し、前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する。

また、第 20 の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記デー

タ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において、前記権利書データの正当性を証明する。

また、第21の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する。

また、第22の発明のデータ提供システムは、データ提供装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

第 2 2 の発明のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給する。

次に、データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。

次に、前記データ処理装置から管理装置に、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを送信する。

次に、前記管理装置において、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第 2 3 の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2 のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第 2 のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配

するための利益分配処理を行う。

第 2 3 の発明のデータ提供システムでは、データ提供装置からデータ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供する。

次に、前記データ配給装置からデータ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給する。

次に、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。

次に、前記データ処理装置から前記管理装置に、前記決定した購入形態および利用形態の履歴を示す履歴データを送信する。

次に、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第 2 4 の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて、前

記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う。

また、第25の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する。

また、第26の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う。

また、第27の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供された

コンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する。

また、第28の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対

応する公開鍵データの公開鍵証明書データを作成および管理するデータ提供システムであって、前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する。

また、第29の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する。

また、第30の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記管理装置は、前記データ

提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する。

また、第31の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給

を制御する。

また、第 3 2 の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けたコンテンツデータを利用する。

また、第 3 3 の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証

明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

また、第34の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

また、第35の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有し、前記管理装置は、前記データ提供装

置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する。

また、第36の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータ

および前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

また、第 37 の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する。

また、第 38 の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登

録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給する。

また、第38の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公

公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

また、第40の発明のデータ提供システムは、データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する。

また、第41の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュール

ルと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有する。

また、第42の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて

決済行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

また、第４３の発明のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置は、前記データ配給装置と通信を行う第１のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第２のモジュールとを有し、前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第２のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する。

また、第４４の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態

の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第45の発明の管理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第46の発明のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信する。

また、第47の発明のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデー

タ配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有する。

また、第48の発明のデータ処理装置は、コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有する。

また、第49の発明のデータ提供方法は、データ提供装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利

用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う。

また、第50の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、前記管理装置において、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う。

また、第51の発明のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権

利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行う。

図面の簡単な説明

図 1 は、本発明の第 1 実施形態の EMD システムの全体構成図である。

図 2 は、図 1 に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークの SAM との間で送受信されるデータに関連するデータの流れを示す図である。

図 3 は、図 1 に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダと EMD サービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

図 4 は、図 1 に示すコンテンツプロバイダから SAM に送信されるセキュアコンテンツのフォーマットを説明するための図である。

図 5 は、OSI レイヤ層と、本実施形態のセキュアコンテンツの定義との対応関係を説明するための図である。

図 6 は、ROM 型の記録媒体を説明するための図である。

図 7 A はコンテンツプロバイダから EMD サービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図 7 B は EMD サービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

図 8 は、第 1 実施形態において、コンテンツプロバイダが、E M D サービスセンタに、自らの秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを要求する場合の処理のフローチャートである。

図 9 は、第 1 実施形態において、コンテンツプロバイダがユーザホームネットワークの S A M にセキュアコンテナを送信する場合の処理のフローチャートである。

図 1 0 は、図 1 に示す E M D サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図 1 1 は、図 1 に示す E M D サービスセンタの機能ブロック図であり、S A M および図 1 に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

図 1 2 は、第 1 実施形態において、E M D サービスセンタがコンテンツプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図 1 3 は、第 1 実施形態において、E M D サービスセンタが S A M から、公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図 1 4 は、第 1 実施形態において、E M D サービスセンタがコンテンツプロバイダから権利書データおよびコンテンツ鍵データの登録要求を受けた場合の処理のフローチャートである。

図 1 5 は、第 1 実施形態において、E M D サービスセンタが決済処理を行なう場合の処理のフローチャートである。

図 1 6 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図である。

図 1 7 は、図 1 に示すユーザホームネットワーク内の S A M の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでの

データの流れを示す図である。

図 1 8 は、図 1 6 に示す外部メモリに記憶されるデータを説明するための図である。

図 1 9 は、スタックメモリに記憶されるデータを説明するための図である。

図 2 0 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

図 2 1 は、図 1 7 に示す記憶部に記憶されるデータを説明するための図である。

図 2 2 は、第 1 実施形態において、セキュアコンテナをコンテンツプロバイダから入力し、セキュアコンテナ内のキーファイル K F を復号する際の S A M 内での処理のフローチャートである。

図 2 3 は、図 1 に示すユーザホームネットワーク内の S A M の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

図 2 4 は、第 1 実施形態において、コンテンツプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの処理のフローチャートである。

図 2 5 は、第 1 実施形態において、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

図 2 6 は、図 1 6 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合の転送元の S A M 内での処理の流れを説明するための図である。

図 2 7 は、図 2 6 に示す場合における転送元の S A M 内でのデータの流れを示す図である。

図 2 8 は、第 1 実施形態において、ネットワーク機器のダウンロードメモリに

ダウンロードされた既に購入形態が決定されたコンテンツファイルおよびキーファイルを、他のAV機器のSAMに転送する場合のSAM内での処理のフローチャートである。

図29は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

図30は、図26に示す場合において、転送先のSAMにおいて、入力したコンテンツファイルなどを、RAM型あるいはROM型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

図31は、第1実施形態において、他のSAMから入力したコンテンツファイルなどを、RAM型などの記録媒体に書き込む際のSAM内での処理のフローチャートである。

図32、コンテンツの購入形態が未決定の図6に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理の流れを説明するための図である。

図33は、図32に示す場合において、SAM内でのデータの流れを示す図である。

図34は、第1実施形態において、コンテンツの購入形態が未決定の図5に示すROM型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV機器において購入形態を決定する際の処理のフローチャートである。

図35は、図34のフローチャートの続きのフローチャートである。

図36は、ユーザホームネットワーク内のAV機器において購入形態が未決定のROM型の記録媒体からセキュアコンテナを読み出して、これを他のAV機器に転送してRAM型の記録媒体に書き込む際の処理の流れを説明するための図である。

図37は、図36に示すように、第1のAV機器において購入形態が未決定の

R O M型の記録媒体からセキュアコンテナを読み出して第2のA V機器に転送し、第2のA V機器において購入形態を決定してR A M型の記録媒体に書き込む際の第1のA V機器の処理のフローチャートである。

図38は、図37に示す場合の第2のA V機器の処理のフローチャートである。

図39は、図38に示すフローチャートの続きのフローチャートである。

図40は、図36に示す場合における転送元のS A M内でのデータの流れを示す図である。

図41は、図36に示す場合における転送先のS A M内でのデータの流れを示す図である。

図42は、図1に示すコンテンツプロバイダ、E M DサービスセンタおよびS A Mの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

図43は、図1に示すコンテンツプロバイダ、E M DサービスセンタおよびS A Mの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

図44は、バスへの機器の接続形態の一例を説明するための図である。

図45は、S A M登録リストのデータフォーマットを説明するための図である。

図46は、図1に示すコンテンツプロバイダの全体動作のフローチャートである。

図47は、本発明の第1実施形態の第2変形例を説明するための図である。

図48は、本発明の第1実施形態の第3変形例を説明するための図である。

図49は、本発明の第2実施形態のE M Dシステムの全体構成図である。

図50は、図49に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図で

ある。

図5 1は、図4 8に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

図5 2は、第2実施形態において、コンテンツプロバイダから供給を受けたセキュアコンテナからセキュアコンテナを作成し、これをユーザホームネットワークに配給する際のサービスプロバイダの処理のフローチャートである。

図5 3は、図4 8に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

図5 4は、図4 8に示すサービスプロバイダの機能ブロック図であり、EMDサービスセンタとの間で送受信されるデータの流れを示す図である。

図5 5は、サービスプロバイダからEMDサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

図5 6は、図4 9に示すEMDサービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図5 7は、図4 9に示すEMDサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

図5 8は、図4 9に示すEMDサービスセンタの機能ブロック図であり、SAMとの間で送受信されるデータに関連するデータの流れを示す図である。

図5 9は、利用履歴データの内容を説明するための図である。

図6 0は、第2実施形態において、EMDサービスセンタがサービスプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

図6 1は、第2実施形態において、EMDサービスセンタが、サービスプロバイダからプライスタグデータの登録要求を受けた場合の処理のフローチャートで

ある。

図 6 2 は、第 2 実施形態において、E M D サービスセンタが決済を行なう場合の処理のフローチャートである。

図 6 3 は、図 4 9 に示すネットワーク機器の構成図である。

図 6 4 は、図 6 3 に示す C A モジュールの機能ブロック図である。

図 6 5 は、図 6 3 に示す S A M の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

図 6 6 は、図 6 5 に示す記憶部に記憶されるデータを説明するための図である。

図 6 7 は、図 6 3 に示す S A M の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

図 6 8 は、第 2 実施形態において、セキュアコンテナをサービスプロバイダから入力し、セキュアコンテナ内のキーファイルを復号する際の S A M の処理のフローチャートである。

図 6 9 は、第 2 実施形態において、サービスプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの S A M の処理のフローチャートである。

図 7 0 は、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

図 7 1 は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

図 7 2 は、図 6 3 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合の転送先の S A M 内での処理の流れを説明するための図である。

図 4 9 は、図 7 2 に示す場合の転送元の S A M 内でのデータの流れを示す図である。

図 7 4 は、図 7 2 に示すように、例えば、ネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合の転送元の S A M の処理のフローチャートである。

図 7 5 は、ネットワーク機器の S A M から A V 機器の S A M に転送される購入形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

図 7 6 は、図 7 2 に示す場合の転送先の S A M 内でのデータの流れを示す図である。

図 7 7 は、図 7 2 に示すように、他の S A M から入力したコンテンツファイルなどを、R A M 型などの記録媒体に書き込む際の S A M の処理のフローチャートである。

図 7 8 は、図 4 9 に示す E M D システムの全体動作のフローチャートである。

図 7 9 は、図 4 9 に示す E M D システムの全体動作のフローチャートである。

図 8 0 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いた E M D システムの構成図である。

図 8 1 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた E M D システムの構成図である。

図 8 2 は、本発明の第 2 実施形態の第 3 変形例に係わる E M D システムの構成図である。

図 8 3 は、本発明の第 2 実施形態の第 4 変形例に係わる E M D システムの構成図である。

図 8 4 は、公開鍵証明書データの取得ルートの形態を説明するための図である。

図 8 5 は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

図 8 6 は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

図 8 7 は、S A M の公開鍵証明書データを無効にする場合の処理を説明するための図である。

図 8 8 は、S A M の公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

図 8 9 は、図 4 9 に示す E M D システムにおいて、E M D サービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

図 9 0 は、図 8 9 に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体の E M D サービスセンタ内に設けた場合の E M D システムの構成図である。

図 9 1 は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の E M D システムの構成図である。

図 9 2 は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の E M D システムの構成図である。

図 9 3 は、本発明の第 2 実施形態の第 8 変形例において、図 4 9 に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

図 9 4 は、図 9 3 に格納されたモジュールの詳細なフォーマットを説明するための図である。

図 9 5 は、本発明の第 2 実施形態の第 8 変形例において、図 4 9 に示すサービスプロバイダから S A M に提供されるセキュアコンテナのフォーマットを説明するための図である。

図 9 6 は、インターネットを用いてセキュアコンテナを提供する場合の概念図である。

図 9 7 は、インターネットを用いてセキュアコンテナを提供する場合のその他の概念図である。

図 9 8 は、デジタル放送を用いてセキュアコンテナを提供する場合の概念図である。

図 9 9 は、デジタル放送を用いてセキュアコンテナを提供する場合のその他の概念図である。

図 1 0 0 は、従来の E M D システムの構成図である。

発明を実施するための最良の形態

以下、本発明の実施形態に係わる E M D (Electronic Music Distribution: 電子音楽配信) システムについて説明する。

本実施形態において、ユーザに配信されるコンテンツ (Content) データとは、音楽データ、映像データおよびプログラムなど情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

第 1 実施形態

図 1 は、本実施形態の E M D システム 1 0 0 の構成図である。

図 1 に示すように、E M D システム 1 0 0 は、コンテンツプロバイダ 1 0 1、E M D サービスセンタ (クリアリング・ハウス、以下、E S C とも記す) 1 0 2 およびユーザホームネットワーク 1 0 3 を有する。

ここで、コンテンツプロバイダ 1 0 1、E M D サービスセンタ 1 0 2 および S A M 1 0 5₁ ~ 1 0 5₄ が、それぞれ本発明のデータ提供装置、管理装置およびデータ処理装置に対応している。

まず、E M D システム 1 0 0 の概要について説明する。

E M D システム 1 0 0 では、コンテンツプロバイダ 1 0 1 は、自らが提供しよ

うとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ102に送信する。権利書データ106は、EMDサービスセンタ102によって権威化(認証)される。

また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成すると共に、コンテンツ鍵データKcをEMDサービスセンタ102から配給された対応する期間の配信用鍵データKD₁～KD₅で暗号化する。そして、コンテンツプロバイダ101は、暗号化されたコンテンツ鍵データKcおよびコンテンツファイルCFと自らの署名データとを格納(カプセル化)したセキュアコンテナ(本発明のモジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク103に配給する。

このように、本実施形態では、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路(配送チャンネル)を介して提供されても、コンテンツデータC(商品)を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module)105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルインタフェースバスなどのバス191を介して接続されている。

SAM105₁～105₄は、ネットワーク機器160₁がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテンツ104、および／または、コンテンツプロバイダ101からAV機器160₂～160₄に記録媒体を介してオフラインで供給されたセキュアコンテンツ104を対応する期間の配信用鍵データKD₁～KD₃を用いて復号した後に、署名データの検証を行う。

SAM105₁～105₄に供給されたセキュアコンテンツ104は、ネットワーク機器160₁およびAV機器160₂～160₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM105₁～105₄は、上述したセキュアコンテンツ104の購入・利用の履歴を利用履歴(Usage Log)データ108として記録する。

利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局82に対しての（ルート認証局82の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM105₁～105₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化することも、EMDサービスセンタ102の認証機能の一つである。

また、EMDサービスセンタ102は、例えば、配信用鍵データKD₁～KD₄などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price)とSAM105₁～SAM105₄から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理（利益分配）機能を有する。

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

〔コンテンツプロバイダ101〕

図2は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM105₁～105₄との間で送受信されるデータに関連するデータの流れが示されている。

また、図3には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。

なお、図3以降の図面では、署名データ処理部、および、セッション鍵データ

K_{SBS} を用いた暗号化・復号部に入出力するデータの流れは省略している。

図2および図3に示すように、コンテンツプロバイダ101は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテンツ作成部118、セキュアコンテンツデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、SAM管理部124およびEMDサービスセンタ管理部125を有する。

コンテンツプロバイダ101は、EMDサービスセンタ102との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでEMDサービスセンタ102に登録し、自らの識別子（識別番号）CP_IDを得る。また、コンテンツプロバイダ101は、EMDサービスセンタ102から、EMDサービスセンタ102の公開鍵データと、ルート認証局92の公開鍵データとを受ける。

以下、図2および図3に示すコンテンツプロバイダ101の各機能ブロックについて説明する。

コンテンツマスタソースサーバ111は、ユーザホームネットワーク103に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータS111を電子透かし情報付加部112に出力する。

電子透かし情報付加部112は、コンテンツデータS111に対して、ソース電子透かし情報(Source Watermark)W_s、コピー管理用電子透かし情報(Copy Control Watermark)W_cおよびユーザ電子透かし情報(User Watermark)W_uなどを埋め込んでコンテンツデータS112を生成し、コンテンツデータS112を圧縮部113に出力する。

ソース電子透かし情報W_sは、コンテンツデータの著作権者名、ISRCコード、オーサリング日付、オーサリング機器ID(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報W

c は、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Wuには、例えば、セキュアコンテナ104の配給元および配給先を特定するためのコンテンツプロバイダ101の識別子CP_IDおよびユーザホームネットワーク103のSAM105₁～105₄の識別子SAM_ID₁～SAM_ID₄が含まれる。

また、電子透かし情報付加部112は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のIDを電子透かし情報としてコンテンツデータS111に埋め込む。

本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、EMDサービスセンタ102において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₄が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

圧縮部113は、コンテンツデータS112を、例えば、ATrac3 (Adaptive Transform Acoustic Coding 3) (商標)などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES (Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。

また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/

V伸長用ソフトウェアS o f tおよびメタデータM e t aを暗号化した後に、セキュアコンテナ作成部117に出力する。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の64ビットは、上位32ビットのH₀と下位32ビットのL₀とに分割される。鍵処理部から供給された48ビットの拡大鍵データK₁および下位32ビットのL₀を入力とし、下位32ビットのL₀を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH₀と、F関数の出力との排他的論理和が算出され、その結果はL₁とされる。また、L₀は、H₁とされる。

そして、上位32ビットのH₀および下位32ビットのL₀を基に、以上の処理を16回繰り返し、得られた上位32ビットのH₁₆および下位32ビットのL₁₆が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データK_cとして暗号化部114および暗号化部116に出力する。

なお、コンテンツ鍵データK_cは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データK_cは、例えば、所定時間毎に更新される。

暗号化部116は、後述するようにしてEMDサービスセンタ102から受信されて記憶部119に記憶された配信用鍵データK_{D1}～K_{Dn}のうち対応する

期間の配信用鍵データ $KD_1 \sim KD_8$ を入力し、当該配信用鍵データを共通鍵として用いた DES などの共通暗号化方式によって図 4 B に示すコンテンツ鍵データ K_c 、権利書データ 106、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_8$ および署名・証明書モジュール Mod_1 を暗号化した後に、セキュアコンテナ作成部 117 に出力する。

署名・証明書モジュール Mod_1 には、図 4 B に示すように、署名データ $SIG_{2, CP} \sim SIG_{4, CP}$ 、コンテンツプロバイダ 101 の公開鍵データ $K_{CP, P}$ の公開鍵証明書 CER_{CP} および当該公開鍵証明書 CER_{CP} に対しての EMD サービスセンタ 102 の署名データ $SIG_{1, BSC}$ が格納されている。

また、SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_8$ は、SAM 105₁ \sim 105₈ 内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ (UCP) U106 のシンタックス (文法) を示す $UCP-L$ (Label) . R (Reader) と、SAM 105₁ \sim 105₈ に内蔵された記憶部 (フラッシュ ROM) の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データとを格納している。

なお、記憶部 118 は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データ $KD_1 \sim KD_8$ を記憶するデータベースおよびキーファイル KF を記憶するデータベースなどの種々のデータベースを備えている。

署名処理部 117 は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ 101 の秘密鍵データ $K_{CP, S}$ を用いて、その署名データ SIG を作成する。

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシ

ュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

セキュアコンテナ作成部 118 は、図 4 A に示すように、ヘッダデータと、暗号化部 114 から入力したそれぞれコンテンツ鍵データ K_c で暗号化されたコンテンツデータ C 、A/V 伸長用ソフトウェア $Soft$ およびメタデータ $Meta$ とを格納したコンテンツファイル CF を生成する。

ここで、A/V 伸長用ソフトウェア $Soft$ は、ユーザホームネットワーク 103 のネットワーク機器 160₁ および AV 機器 160₂ ~ 160₄ において、コンテンツファイル CF を伸長する際に用いられるソフトウェアであり、例えば、ATRAC3 方式の伸長用ソフトウェアである。

また、セキュアコンテナ作成部 118 は、図 4 B に示すように、暗号化部 116 から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_8$ で暗号化されたコンテンツ鍵データ K_c 、権利書データ (UCP) 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_8$ および署名・証明書モジュール Mod_1 を格納したキーファイル KF を生成する。

そして、セキュアコンテナ作成部 118 は、図 4 A, B に示すコンテンツファイル CF およびキーファイル KF と、図 4 C に示すコンテンツプロバイダ 101 の公開鍵データ K_{CP} および署名データ SIG_{1_BSC} とを格納したセキュアコンテナ 104 を生成し、これをセキュアコンテナデータバス 118a に格納した後に、ユーザからの要求に応じて SAM 管理部 124 に出力する。

このように、本実施形態では、コンテンツプロバイダ 101 の公開鍵データ K_{CP} の公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納してユーザホームネットワーク 103 に送信するイン・バンド (In-band) 方式を採用している。従って、ユーザホームネットワーク 103 は、公開鍵証明書 CER_{CP} を得るための通信を EMD サービスセンタ 102 との間で行う必要がない。

なお、本発明では、公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納しないで、ユーザホームネットワーク 103 が EMD サービスセンタ 102 から公

開鍵証明書 CER_{cp} を得るアウト・オブ・バンド (Out-Of-band) 方式を採用してもよい。

相互認証部 120 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 との間でオンラインでデータを送受信する際に、それぞれ EMD サービスセンタ 102 およびユーザホームネットワーク 103 との間で相互認証を行ってセッション鍵データ (共有鍵) K_{sbs} を生成する。セッション鍵データ K_{sbs} は、相互認証を行う度に新たに生成される。

暗号化・復号部 121 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 にオンラインで送信するデータを、セッション鍵データ K_{sbs} を用いて暗号化する。

また、暗号化・復号部 121 は、コンテンツプロバイダ 101 が EMD サービスセンタ 102 およびユーザホームネットワーク 103 からオンラインで受信したデータを、セッション鍵データ K_{sbs} を用いて復号する。

権利書データ作成部 122 は、権利書データ 106 を作成し、これを暗号化部 116 に出力する。

権利書データ 106 は、コンテンツデータ C の運用ルールを定義した記述子 (ディスクリプター) であり、例えば、コンテンツプロバイダ 101 の運用者が希望する標準小売価格 SRP (Suggested Retailer' Price) やコンテンツデータ C の複製ルールなどが記述されている。

SAM 管理部 124 は、セキュアコンテナ 104 を、オフラインおよび/またはオンラインでユーザホームネットワーク 103 に供給する。

SAM 管理部 124 は、CD-ROM や DVD (Digital Versatile Disc) などの ROM 型の記録媒体 (メディア) を用いてセキュアコンテナ 104 をオフラインでユーザホームネットワーク 103 に配給する場合には、配信用鍵データ $KD_1 \sim KD_n$ などを用いてセキュアコンテナ 104 を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク 10

3にオフラインで供給される。

本実施形態では、セキュアコンテナ（商品カプセル）104は、図5に示すように、OS Iレイヤ層におけるアプリケーション層で定義される。また、プレゼンテーション層やトランスポート層に相当するカプセルは、セキュアコンテナを配送するための配送プロトコルとして、セキュアコンテナ104とは別に定義される。従って、セキュアコンテナ104を配送プロトコルに依存しないで定義できる。すなわち、セキュアコンテナ104を、例えばオンラインおよびオフラインの何れの形態でユーザホームネットワーク103に供給する場合でも、共通のルールに従って定義および生成できる。

例えば、セキュアコンテナ104をネットワークを使って供給する場合には、セキュアコンテナ104をコンテンツプロバイダ101の領域で定義し、プレゼンテーション層およびトランスポート層をセキュアコンテナ104をユーザホームネットワーク103まで搬送するための搬送ツールと考える。

また、オフラインの場合に、ROM型の記録媒体を、セキュアコンテナ104をユーザホームネットワーク103に搬送する搬送キャリアとして考える。

図6は、ROM型の記録媒体130を説明するための図である。

図6に示すように、ROM型の記録媒体130は、ROM領域131、RAM領域132およびメディアSAM133を有する。

ROM領域131には、図4Aに示したコンテンツファイルCFが記憶されている。

また、RAM領域132には、図4B、図4Cに示したキーファイルKFおよび公開鍵証明書データCER_{CP}と機器の種類に応じて固有の値を持つ記録用鍵データK_{STR}とを引数としてMAC(Message Authentication Code)関数を用いて生成したと署名データと、当該キーファイルKFおよび公開鍵証明書データCER_{CP}とを記録媒体に固有の値を持つメディア鍵データK_{MED}を用いて暗号化したデータとが記憶される。

また、RAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM105₁～105₄を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

また、また、RAM領域132には、後述するようにユーザホームネットワーク103のSAM105₁～105₄においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態（UCS）データ166などが記憶される。これにより、利用制御状態データ166がRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130となる。

メディアSAM133には、例えば、ROM型の記録媒体130の識別子であるメディアIDと、メディア鍵データK_{MBD}とが記憶されている。

メディアSAM133は、例えば、相互認証機能を有している。

また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データK_{SES}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。

本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM105₁～105₄では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を

行なうことができる。

また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データ K_c で暗号化されたコンテンツデータ C と、当該暗号化を解くためのコンテンツ鍵データ K_c とを同封するイン・バンド(In-Band)方式を採用している。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータ C を再生しようとするときに、コンテンツ鍵データ K_c を別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データ K_c は配信用鍵データ $KD_1 \sim KD_8$ で暗号化されているが、配信用鍵データ $KD_1 \sim KD_8$ は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103の $SAM105_1 \sim 105_8$ に事前に($SAM105_1 \sim 105_8$ がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータ C の利用が可能になる。

なお、本発明は、コンテンツデータ C とコンテンツ鍵データ K_c とを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

EMDサービスセンタ管理部125は、EMDサービスセンタ102から6カ月分の配信用鍵データ $KD_1 \sim KD_8$ およびそれぞれに対応した署名データ $SIG_{KD1,ESC} \sim SIG_{KD8,ESC}$ と、コンテンツプロバイダ101の公開鍵データ $K_{CP,P}$ を含む公開鍵証明書 CER_{CP} およびその署名データ $SIG_{1,ESC}$ と、決済レポートデータ107とを受信すると、これらを暗号化・復号部121においてセッション鍵データ K_{SES} を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique)な識別子Content_ID、公開鍵データ $K_{CP, P}$ およびそれらの署名データ $SIG_{S, CP}$ を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データ $K_{CP, P}$ の公開鍵証明書データ CER_{CP} を入力する。

また、EMDサービスセンタ管理部125は、権利書データ106をEMDサービスセンタ102に登録する際に、図7Aに示すように、提供するコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データ K_C および権利書データ106を格納したモジュール Mod_1 と、その署名データ $SIG_{S, CP}$ とを格納した権利書登録要求用モジュール Mod_2 を作成し、これを暗号化・復号部121においてセッション鍵データ K_{SSS} を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

以下、図2および図3を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶される。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データ $K_{CP, S}$ に対応する公開鍵データ $K_{CP, S}$ の正当性を証明する公開鍵証明書データ CER_{CP} を要求する場合の処理を図3および図8を参照しながら説明する。

図8は、当該処理のフローチャートである。

ステップSA1：コンテンツプロバイダ101は、例えば真性乱数発生器から構成される乱数発生部115を用いて乱数を発生して秘密鍵データ $K_{CP, s}$ を生成する。

ステップSA2：コンテンツプロバイダ101は、秘密鍵データ $K_{CP, s}$ に対応する公開鍵データ $K_{CP, p}$ を作成して記憶部119に記憶する。

ステップSA3：コンテンツプロバイダ101のEMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子 CP_ID および公開鍵データ $K_{CP, p}$ を記憶部119から読み出す。

そして、EMDサービスセンタ管理部125は、識別子 CP_ID および公開鍵データ $K_{CP, p}$ を含む公開鍵証明書データ発行要求をEMDサービスセンタ102に送信する。

ステップSA4：EMDサービスセンタ管理部125は、当該発行要求に応じて、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1, BSC}$ をEMDサービスセンタ102から入力して記憶部119に書き込む。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102から配信用鍵データを受信する処理を図3を参照しながら説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101は、EMDサービスセンタ102から既に公開鍵証明書データ CER_{CP} を得ている必要がある。

EMDサービスセンタ管理部125が、EMDサービスセンタ102から6カ月分の配信用鍵データ $KD_1 \sim KD_9$ およびその署名データ $SIG_{KD1, BSC} \sim SIG_{KD8, BSC}$ を入力し、これを記憶部119内の所定のデータベースに記憶する。

そして、署名処理部117において、記憶部119に記憶された署名データ $SIG_{KD1, BSC} \sim SIG_{KD8, BSC}$ の正当性が確認された後に、記憶部119に記憶

されている配信用鍵データ $KD_1 \sim KD_8$ が有効なものとして扱われる。

以下、コンテンツプロバイダ 101 がユーザホームネットワーク 103 の $SAM105_1$ にセキュアコンテナ 104 を送信する場合の処理を図 2 および図 8 を参照しながら説明する。

図 8 は、当該処理のフローチャートである。

なお、以下の例では、コンテンツプロバイダ 101 から $SAM105_1$ にセキュアコンテナ 104 を送信する場合を例示するが、セキュアコンテナ 104 を $SAM105_2 \sim 105_4$ に送信する場合も、 $SAM105_1$ を介して $SAM105_2 \sim 105_4$ に送信される点を除いて同じである。

ステップ SB1 : コンテンツデータ S111 がコンテンツマスタソースサーバ 111 から読み出されて電子透かし情報付加部 112 に出力される。

電子透かし情報付加部 112 は、コンテンツデータ S111 に電子透かし情報を埋め込んでコンテンツデータ S112 を生成し、これを圧縮部 113 に出力する。

ステップ SB2 : 圧縮部 113 は、コンテンツデータ S112 を、例えば AT RAC3 方式で圧縮してコンテンツデータ S113 を作成し、これを暗号化部 114 に出力する。

ステップ SB3 : 乱数発生部 115 は、乱数を発生してコンテンツ鍵データ K_c を生成し、これを暗号化部 114 に出力する。

ステップ SB4 : 暗号化部 114 は、コンテンツデータ S113 と、記憶部 119 から読み出されたメタデータ $Meta$ および A/V 伸長用ソフトウェア $Soft$ とを、コンテンツ鍵データ K_c を用いて暗号化してセキュアコンテナ作成部 118 に出力する。この場合に、メタデータ $Meta$ は暗号化しなくてもよい。

そして、セキュアコンテナ作成部 118 は、図 4 A に示すコンテンツファイル CF を作成する。また、署名処理部 117 において、コンテンツファイル CF の

ハッシュ値がとられ、秘密鍵データ $K_{CP, s}$ を用いて署名データ $SIG_{8, CP}$ が生成される。

ステップSB5：署名処理部117は、コンテンツデータC、コンテンツ鍵データ K_C および権利書データ106のそれぞれに対してハッシュ値をとり、秘密鍵データ $K_{CP, s}$ を用いて、それぞれのデータの作成者（提供者）の正当性を示す署名データ $SIG_{2, CP}$, $SIG_{3, CP}$, $SIG_{4, CP}$ を作成する。

また、暗号化部116は、図4Bに示すコンテンツ鍵データ K_C 、権利書データ106、SAMプログラム・ダウンロード・コンテナ $SD_1 \sim SD_9$ および署名・証明書モジュール Mod_1 を、対応する期間の配信用鍵データ $KD_1 \sim KD_9$ で暗号化してセキュアコンテナ作成部118に出力する。

そして、セキュアコンテナ作成部118は、図4Bに示すキーファイルKFを作成する。

また、署名処理部117は、キーファイルKFのハッシュ値をとり、秘密鍵データ $K_{CP, s}$ を用いて、署名データ $SIG_{7, CP}$ を作成する。

ステップSB6：セキュアコンテナ作成部118は、図4Aに示すコンテンツファイルCFおよびその署名データ $SIG_{8, CP}$ と、図4Bに示すキーファイルKFおよびその署名データ $SIG_{7, CP}$ と、図4Cに示す公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1, BSC}$ とを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。

ステップSB7：セキュアコンテナ作成部118は、例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118aから読み出して、相互認証部120とSAM105₁との間の相互認証によって得られたセッション鍵データ K_{SSS} を用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM105₁に送信する。

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に権利書データ106およびコンテンツ鍵データKcを登録して権威化することを要求する場合の処理を図3を参照して説明する。

権利書データ106およびコンテンツ鍵データKcの権威化要求処理は、個々のコンテンツデータC毎に行われる。

この場合には、署名処理部117において、記憶部119から読み出したコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106からなるモジュールMod₁のハッシュ値が求められ、秘密鍵データK_{CP,s}を用いて署名データSIG_{s,CP}が生成される。

そして、図7Aに示す権利登録要求用モジュールMod₂を、相互認証部120とEMDサービスセンタ102との間の相互認証によって得られたセッション鍵データK_{SSS}を用いて暗号化・復号部121において暗号化した後に、EMDサービスセンタ管理部125からEMDサービスセンタ102に送信する。

本実施形態では、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、コンテンツプロバイダ101がEMDサービスセンタ102から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ101において配信用鍵データKD₁～KD₈を用いて暗号化を行ってキーファイルKFを作成する場合を例示する。

但し、本発明は、例えば、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、配信用鍵データKD₁～KD₈を用いて暗号化した図7Bに示す権威化証明書モジュールMod_{2a}を送信してもよい。

権威化証明書モジュールMod_{2a}は、コンテンツデータCのグローバルユニーク

クな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106を格納したモジュールMod_{sa}と、秘密鍵データK_{esc, s}を用いたモジュールMod_{sa}の署名データSIG_{sa, esc}とを格納している。

この場合には、コンテンツプロバイダ101は、例えば、セキュアコンテナ104内に、権威化証明書モジュールMod_zを格納してSAM105₁～105₄に配給する。

なお、EMDサービスセンタ102は、それぞれ異なる月に対応する配信用鍵データKD₁～KD₈を用いて暗号化した6カ月分の権威化証明書モジュールMod_zを生成し、これらをまとめてコンテンツプロバイダ101に送信してもよい。

〔EMDサービスセンタ102〕

EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing) (利益分配)機能を有する。

図10は、EMDサービスセンタ102の機能の構成図である。

図10に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、CERデータベース145a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部148、SAMデータベース149a、相互認証部150および暗号化・復号部151を有する。

なお、図10には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流れが示されている。

また、図11には、EMDサービスセンタ102内の機能ブロック相互間のデ

ータの流れのうち、SAM105₁～105₄および図1に示す決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部148およびSAM管理部149に出力する。

また、鍵データベース141a配信用鍵データKDの他に、記録用鍵データK_{STR}、メディア鍵データK_{MBD}およびMAC鍵データK_{MAC}などの鍵データを記憶する一連の鍵データスからなる。

決算処理部142は、SAM105₁～105₄から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144に出力する。

なお、決算処理部142は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ108は、ユーザホームネットワーク103におけるセキュアコンテナ104の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部142においてセキュアコンテナ104に関連したライセンス料の支払い額を決定する際に用いられる。

利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105₁～105₄の識別子SAM_ID、当該SAM105₁～105₄のユ

ーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテンツ104に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関91は、決済が終了すると、当該決済機関の利用明細書をEMDサービスセンタ102に送る。EMDサービスセンタ102は、当該利用明細書の内容を、対応する権利者に通知する。

決算機関管理部144は、決算処理部142が生成した決済請求権データ152を図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

なお、後述するように、決算機関管理部144は、決済請求権データ152を、コンテンツプロバイダ101などの権利者に送信し、権利者自らが、受信した決済請求権データ152を用いて決済機関91に決済を行ってもよい。

また、決算機関管理部144は、署名処理部143において決済請求権データ152のハッシュ値をとり、秘密鍵データ $K_{ESC,s}$ を用いて生成した署名データ SIG_{ss} を決済請求権データ152と共に決済機関91に送信する。

証明書・権利書管理部145は、CERデータベース145aに登録されて権威化された公開鍵証明書データ CER_{cp} および公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ などを読み出すと共に、コンテンツプロバイダ101の権利書データ106およびコンテンツ鍵データ K_c などをCERデータベース145aに登録

して権威化する。

なお、公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を格納するデータベースと、権利書データ 106 およびコンテンツ鍵データ K_c とを個別に設けてもよい。

このとき、証明書・権利書管理部 145 は、例えば、権利書データ 106 およびコンテンツ鍵データ K_c などのハッシュ値をとり、秘密鍵データ $K_{ESC, S}$ を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されたコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

SAM 管理部 149 は、ユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ との間で通信する機能を有し、登録された SAM の識別子 SAM_ID や SAM 登録リストなどを記録した SAM データベース 149a にアクセスできる。

以下、 EMD サービスセンタ 102 内での処理の流れを説明する。

まず、 EMD サービスセンタ 102 からコンテンツプロバイダ 101 およびユーザホームネットワーク 103 内の $SAM105_1 \sim 105_4$ への配信用鍵データを送信する際の処理の流れを、図 10 および図 11 を参照しながら説明する。

図 10 に示すように、鍵サーバ 141 は、所定期間毎に、例えば、6 カ月分の配信用鍵データ $KD_1 \sim KD_8$ を鍵データベース 141a から読み出してコンテンツプロバイダ管理部 148 に出力する。

また、署名処理部 143 は、配信用鍵データ $KD_1 \sim KD_8$ の各々のハッシュ値をとり、 EMD サービスセンタ 102 の秘密鍵データ $K_{ESC, S}$ を用いて、それぞれに対応する署名データ $SIG_{KD1, ESC} \sim SIG_{KD8, ESC}$ を作成し、これをコンテンツプロバイダ管理部 148 に出力する。

コンテンツプロバイダ管理部148は、この6カ月分の配信用鍵データ $KD_1 \sim KD_6$ およびそれらの署名データ $SIG_{KD_1, BSC} \sim SIG_{KD_6, BSC}$ を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SBS} を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

また、図11に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データ $KD_1 \sim KD_3$ を鍵データベース141aから読み出してSAM管理部149に出力する。

また、署名処理部143は、配信用鍵データ $KD_1 \sim KD_3$ の各々のハッシュ値を取り、EMDサービスセンタ102の秘密鍵データ $K_{BSC, S}$ を用いて、それぞれに対応する署名データ $SIG_{KD_1, BSC} \sim SIG_{KD_3, BSC}$ を作成し、これをSAM管理部149に出力する。

SAM管理部149は、この3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびそれらの署名データ $SIG_{KD_1, BSC} \sim SIG_{KD_3, BSC}$ を、相互認証部150とSAM105₁～105₄と間の相互認証で得られたセッション鍵データ K_{SBS} を用いて暗号化した後に、SAM105₁～105₄に送信する。

以下、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データ CER_{CP} の発行要求を受けた場合の処理を、図10および図12を参照しながら説明する。

図12は、当該処理のフローチャートである。

ステップSC1：コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子 CP_ID 、公開鍵データ $K_{CP, P}$ および署名データ $SIG_{g, CP}$ を含む公開鍵証明書データ発行要求をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SBS} を用いて復号する。

ステップSC2：当該復号した署名データ $SIG_{g, CP}$ の正当性を署名処理部1

43において確認した後に、識別子 CP_ID および公開鍵データ $K_{CP,P}$ に基づいて、当該公開鍵証明書データ発行要求を出したコンテンツプロバイダ101が CP データベース148aに登録されているか否かを確認する。

ステップSC3：証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データ CER_{CP} を CER データベース145aから読み出してコンテンツプロバイダ管理部148に出力する。

ステップSC4：署名処理部143は、公開鍵証明書データ CER_{CP} のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{1,ESC}$ を作成し、これをコンテンツプロバイダ管理部148に出力する。

ステップSC5：コンテンツプロバイダ管理部148は、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

以下、EMDサービスセンタ102が $SAM105_1$ から、公開鍵証明書データ CER_{SAM1} の発行要求を受けた場合の処理を、図11および図13を参照しながら説明する。

図13は、当該処理のフローチャートである。

ステップSD1：SAM管理部149は、 $SAM105_1$ の識別子 $SAM1_ID$ 、公開鍵データ $K_{SAM1,P}$ および署名データ $SIG_{8,SAM1}$ を含む公開鍵証明書データ発行要求を $SAM105_1$ から受信すると、これらを、相互認証部150と $SAM105_1$ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

ステップSD2：当該復号した署名データ $SIG_{8,SAM1}$ の正当性を署名処理部143において確認した後に、識別子 $SAM1_ID$ および公開鍵データ $K_{SAM1,P}$ に基づいて、当該公開鍵証明書データの発行要求を出した $SAM105_1$ がS

AMデータベース149aに登録されているか否かを確認する。

ステップSD3：証明書・権利書管理部145は、当該SAM105₁の公開鍵証明書データCER_{SAM1}をCERデータベース145aから読み出してSAM管理部149に出力する。

ステップSD4：署名処理部143は、公開鍵証明書データCER_{SAM1}のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{BSC, s}を用いて、署名データSIG_{50, BSC}を作成し、これをSAM管理部149に出力する。

ステップSD5：SAM管理部149は、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{50, BSC}を、相互認証部150とSAM105₁と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM105₁に送信する。

なお、SAM105₂～105₄が、公開鍵証明書データを要求した場合の処理は、対象がSAM105₂～105₄に代わるのみで、基本的に上述したSAM105₁の場合と同じである。

なお、本発明では、EMDサービスセンタ102は、例えば、SAM105₁の出荷時に、SAM105₁の秘密鍵データK_{SAM1, s}および公開鍵データK_{SAM1, p}をSAM105₁の記憶部に記憶する場合には、当該出荷時に、公開鍵データK_{SAM1, p}の公開鍵証明書データCER_{SAM1}を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データCER_{SAM1}を、SAM105₁の記憶部に記憶してもよい。

以下、EMDサービスセンタ102が、コンテンツプロバイダ101から権利書データ106およびコンテンツ鍵データK_cの登録要求を受けた場合の処理を、図10および図14を参照しながら説明する。

図14は、当該処理のフローチャートである。

ステップSE1：コンテンツプロバイダ管理部148は、コンテンツプロバイダ101から図7Aに示す権利書登録要求モジュールMod₂を受信すると、相

相互認証部 150 と図 3 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{SBS} を用いて権利書登録要求モジュール Mod_2 を復号する。

ステップ SE 2 : 署名処理部 143 において、鍵データベース 141a から読み出した公開鍵データ K_{cp} を用いて、署名データ $SIG_{s, cp}$ の正当性を検証する。

ステップ SE 3 : 証明書・権利書管理部 145 は、権利書登録要求モジュール Mod_2 に格納された権利書データ 106 およびコンテンツ鍵データ K_c を、CER データベース 145a に登録する。

以下、EMD サービスセンタ 102 において決済処理を行なう場合の処理を図 11 および図 15 を参照しながら説明する。

図 15 は、当該処理のフローチャートである。

ステップ SF 1 : SAM 管理部 149 は、ユーザホームネットワーク 103 の例えば SAM 105₁ から利用履歴データ 108 およびその署名データ $SIG_{200, SAM1}$ を入力すると、利用履歴データ 108 および署名データ $SIG_{200, SAM1}$ を、相互認証部 150 と SAM 105₁ との間の相互認証によって得られたセッション鍵データ K_{SBS} を用いて復号し、SAM 105₁ の公開鍵データ K_{SAM1} による署名データ $SIG_{200, SAM1}$ の検証を行なった後に、決算処理部 142 に出力する。

ステップ SF 2 : 決算処理部 142 は、SAM 管理部 149 から入力した利用履歴データ 108 と、証明書・権利書管理部 145 を介して CER データベース 145a から読み出した権利書データ 106 に含まれる標準小売価格データ SRP および販売価格とに基づいて決済処理を行い、決済請求権データ 152 および決済レポートデータ 107 を生成する。なお、決済請求権データ 152 および決済レポートデータ 107 の生成は、SAM から利用履歴データ 108 を入力する度に行ってもよいし、所定の期間毎に行ってもよい。

ステップ SF 3 : 決算処理部 142 は、決済請求権データ 152 を決算機関管

理部 144 に出力する。

決算機関管理部 144 は、決済請求権データ 152 およびその署名データ SIG_{ss} を、相互認証およびセッション鍵データ K_{ss} による復号を行なった後に、図 1 に示すペイメントゲートウェイ 90 を介して決済機関 91 に送信する。

これにより、決済請求権データ 152 に示される金額の金銭が、コンテンツプロバイダ 101 に支払われる。

なお、EMD サービスセンタ 102 は、決済請求権データ 152 をコンテンツプロバイダ 101 に送信し、コンテンツプロバイダ 101 が決済請求権データ 152 を用いて決済記載 91 に金銭を請求してもよい。

ステップ SF4: 決算処理部 142 は、決済レポートデータ 107 をコンテンツプロバイダ管理部 148 に出力する。

決済レポートデータ 107 は、上述したように、例えば、EMD サービスセンタ 102 が図 1 に示す決済機関 91 に対して行なったコンテンツプロバイダ 101 に関する決済の内容が記述されている。

コンテンツプロバイダ管理部 148 は、決済レポートデータ 107 を、相互認証部 150 と図 3 に示す相互認証部 120 と間の相互認証で得られたセッション鍵データ K_{ss} を用いて暗号化した後に、コンテンツプロバイダ 101 に送信する。

また、EMD サービスセンタ 102 は、前述したように、権利書データ 106 を登録（権威化）した後に、EMD サービスセンタ 102 からコンテンツプロバイダ 101 に、図 7B に示す権威化証明書モジュール Mod_a を配信用鍵データ $KD_1 \sim KD_n$ で暗号化して送信してもよい。

また、EMD サービスセンタ 102 は、その他に、 $SAM_{105_1} \sim 105_n$ の出荷時の処理と、SAM 登録リストの登録処理とを行なうが、これらの処理については後述する。

〔ユーザホームネットワーク 103〕

ユーザホームネットワーク 103 は、図 1 に示すように、ネットワーク機器 160₁ および A/V 機器 160₂ ~ 160₄ を有している。

ネットワーク機器 160₁ は、SAM105₁ を内蔵している。また、AV 機器 160₂ ~ 160₄ は、それぞれ SAM105₂ ~ 105₄ を内蔵している。

SAM105₁ ~ 105₄ の相互間は、例えば、IEEE 1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、AV 機器 160₂ ~ 160₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 160₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 103 は、ネットワーク機能を有していない AV 機器のみを有していてもよい。

以下、ネットワーク機器 160₁ について説明する。

図 16 ネットワーク機器 160₁ の構成図である。

図 16 に示すように、ネットワーク機器 160₁ は、SAM105₁、通信モジュール 162、復号・伸長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

SAM105₁ ~ 105₄ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMD サービスセンタ 102 との間で通信を行う。

SAM105₁ ~ 105₄ は、例えば、EMD サービスセンタ 102 によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁ ~ 105₄ の IC (Integrated Circuit) の内部の仕様を知ることはできず、EMD サービスセンタ 102 が当該 IC のインタフェースなどを統一化し、それに従ってネット

ワーク機器160₁、およびAV機器160₂～160₄に搭載される。

SAM105₁～105₄は、その処理内容が外部から完全に遮断され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)である。

SAM105₁～105₄の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

以下、SAM105₁の機能について詳細に説明する。

なお、SAM105₂～105₄は、SAM105₁と基本的に同じ機能を有している。

図17は、SAM105₁の機能の構成図である。

なお、図17には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流が示されている。

図17に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック(作業)メモリ200および外部メモリ管理部811を有する。

なお、AV機器160₂～160₄はダウンロードメモリ167を有していないため、SAM105₂～105₄にはダウンロードメモリ管理部182は存在

しない。

なお、図17に示すSAM105₁の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。

また、スタックメモリ200には、以下に示す処理を経て、図18に示すように、利用履歴データ108およびSAM登録リストが記憶される。

ここで、外部メモリ201のメモリ空間は、SAM105₁の外部（例えば、ホストCPU810）からは見ることはできず、SAM105₁のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。

外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、スタックメモリ200としては、例えばSARAMが用いられ、図19に示すように、セキュアコンテナ104、コンテンツ鍵データK_c、権利書データ（UCP）106、記憶部192のロック鍵データK_{Loc}、コンテンツプロバイダ101の公開鍵証明書CER_{CP}、利用制御状態データ（UCS）166、およびSAMプログラム・ダウンロード・コンテナSDC₁～SDC₈などが記憶される。

以下、SAM105₁の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図17を参照しながら説明する。

相互認証部170は、SAM105₁がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成し、これを暗号化・復号部171に出力する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービス

センタ 102 との間で送受信するデータを、相互認証部 170 が生成したセッション鍵データ K_{SES} を用いて暗号化・復号する。

誤り訂正部 181 は、セキュアコンテナ 104 を誤り訂正してダウンロードメモリ管理部 182 に出力する。

なお、ユーザホームネットワーク 103 は、セキュアコンテナ 104 が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部 181 を、SAM105₁ に内蔵した場合を例示したが、誤り訂正部 181 の機能を、例えばホスト CPU 810 などの SAM105₁ の外部に持たせてもよい。

ダウンロードメモリ管理部 182 は、図 16 に示すようにダウンロードメモリ 167 が相互認証機能を持つメディア SAM167_a を有している場合には、相互認証部 170 とメディア SAM167_a との間で相互認証を行った後に、誤り訂正後のセキュアコンテナ 104 を、相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化して図 16 に示すダウンロードメモリ 167 に書き込む。ダウンロードメモリ 167 としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図 20 に示すように、HDD (Hard Disk Drive) などの相互認証機能を備えていないメモリをダウンロードメモリ 211 として用いる場合には、ダウンロードメモリ 211 内はセキュアではないので、コンテンツファイル CF をダウンロードメモリ 211 にダウンロードし、機密性の高いキーファイル KF を例えば、図 17 に示すスタックメモリ 200 にダウンロードする。

セキュアコンテナ復号部 183 は、ダウンロードメモリ管理部 182 から入力したセキュアコンテナ 104 に格納されたキーファイル KF を、記憶部 192 から読み出した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号し、署名処理部 189 において署名データ $SIG_{2, CP} \sim SIG_{4, CP}$ の正当性、すなわちコンテンツデータ C、コンテンツ鍵データ K_c および権利書データ 106 の作成

者の正当性を確認した後、スタックメモリ200に書き込む。

EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ およびコンテンツプロバイダ101の公開鍵データ $K_{CP, P}$ を用いて、セキュアコンテナ104内の署名データの検証を行なう。

記憶部192は、SAM105₁の外部から読み出しおよび書き換えできない秘密データとして、図21に示すように、配信用鍵データ $KD_1 \sim KD_s$ 、SAM_ID、ユーザID、パスワード、情報参照用ID、SAM登録リスト、記録用鍵データ K_{STR} 、ルートCAの公開鍵データ $K_{R-CA, P}$ 、EMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ 、メディア鍵データ K_{MED} 、EMDサービスセンタ102の公開鍵データ $K_{ESC, P}$ 、SAM105₁の秘密鍵データ $K_{SAM1, S}$ 、SAM105₁の公開鍵データ $K_{SAM1, P}$ を格納した公開鍵証明書 CER_{SAM1} 、EMDサービスセンタ102の秘密鍵データ $K_{ESC, S}$ を用いた公開鍵証明書 CER_{ESC} の署名データ SIG_{22} 、復号・伸長モジュール163との間の相互認証用の元鍵データ、メディアSAMとの間の相互認証用の元鍵データを記憶している。

また、記憶部192には、図17に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

以下、SAM105₁の処理の流れのうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの処理の流れを説明する。

まず、EMDサービスセンタ102から受信した配信用鍵データ $KD_1 \sim KD_s$ を記憶部192に格納する際のSAM105₁内での処理の流れを図17を参照しながら説明する。

この場合には、まず、相互認証部170と図10に示す相互認証部150との

間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ K_{SES} で暗号化された3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1, BSC} \sim SIG_{KD3, BSC}$ が、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。

次に、暗号化・復号部171において、セッション鍵データ K_{SES} を用いて、配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1, BSC} \sim SIG_{KD3, BSC}$ が復号される。

次に、署名処理部189において、スタックメモリ811に記憶された署名データ $SIG_{KD1, BSC} \sim SIG_{KD3, BSC}$ の正当性が確認された後に、配信用鍵データ $KD_1 \sim KD_3$ が記憶部192に書き込まれる。

以下、セキュアコンテナ104をコンテンツプロバイダ101から入力し、セキュアコンテナ104内のキーファイルKFを復号する際のSAM1051内での処理の流れを図17および図22を参照しながら説明する。

図22は、当該処理のフローチャートである。

ステップSG1：図17に示すSAM1051の相互認証部170と図2に示す相互認証部120との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、コンテンツプロバイダ管理部180を介してコンテンツプロバイダ101から受信したセキュアコンテナ104を復号する。

ステップSG2：署名処理部189は、図4Cに示す署名データ $SIG_{1, BSC}$ の検証を行なった後に、図4Cに示す公開鍵証明書データ CER_{CP} 内に格納されたコンテンツプロバイダ101の公開鍵データ $K_{CP, P}$ を用いて、署名データ $SIG_{8, CP}$, $SIG_{7, CP}$ の正当性を確認する。

コンテンツプロバイダ管理部180は、署名データ $SIG_{8, CP}$, $SIG_{7, CP}$ の正当性が確認されると、セキュアコンテナ104を誤り訂正部181に出力する

。誤り訂正部 181 は、セキュアコンテナ 104 を誤り訂正した後に、ダウンロードメモリ管理部 182 に出力する。

ステップ SG 3 : ダウンロードメモリ管理部 182 は、相互認証部 170 と図 16 に示すメディア SAM 167a との間で相互認証を行なった後に、セキュアコンテナ 104 をダウンロードメモリ 167 に書き込む。

ステップ SG 4 : ダウンロードメモリ管理部 182 は、相互認証部 170 と図 16 に示すメディア SAM 167a との間で相互認証を行なった後に、セキュアコンテナ 104 に格納された図 4B に示すキーファイル KF をダウンロードメモリ 167 から読み出してセキュアコンテナ復号部 183 に出力する。

そして、セキュアコンテナ復号部 183 は、記憶部 192 から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイル KF を復号し、図 4B に示す署名・証明書モジュール Mod_1 に格納された署名データ $SIG_{1, BSC}$ 、 $SIG_{2, CP} \sim SIG_{4, CP}$ を署名処理部 189 に出力する。

ステップ SG 5 : 署名処理部 189 は、図 4B に示す署名データ $SIG_{1, BSC}$ の検証を行なった後に、図 4B に示す公開鍵証明書データ CER_{CP} 内に格納された公開鍵データ $K_{BSC, P}$ を用いて署名データ $SIG_{2, CP} \sim SIG_{4, CP}$ の検証を行なう。これにより、コンテンツデータ C、コンテンツ鍵データ K_C および権利書データ 106 の作成者の正当性が検証される。

ステップ SG 6 : セキュアコンテナ復号部 183 は、署名データ $SIG_{2, CP} \sim SIG_{4, CP}$ の正当性が確認されると、キーファイル KF をスタックメモリ 200 に書き込む。

以下、ダウンロードメモリ 167 にダウンロードされたコンテンツデータ C を利用・購入する処理に関連する各機能ブロックの処理内容を図 23 を参照しながら説明する。

利用監視部 186 は、スタックメモリ 200 から権利書データ 106 および利

利用制御状態データ 166 を読み出し、当該読み出した権利書データ 106 および利用制御状態データ 166 によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ 106 は、図 17 を用いて説明したように、復号後にスタックメモリ 200 に記憶された図 4 B に示すキーファイル KF 内に格納されている。

また、利用制御状態データ 166 は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ 200 に記憶される。

課金処理部 187 は、図 16 に示す購入・利用形態決定操作部 165 からの操作信号 S165 に応じた利用履歴データ 108 を作成する。

ここで、利用履歴データ 108 は、前述したように、ユーザによるセキュアコンテナ 104 の購入および利用の形態の履歴を記述しており、EMD サービスセンタ 102 において、セキュアコンテナ 104 の購入に応じた決済処理およびラインセンス料の支払いを決定する際に用いられる。

また、課金処理部 187 は、必要に応じて、スタックメモリ 200 から読み出した販売価格あるいは標準小売価格データ SRP をユーザに通知する。

ここで、販売価格および標準小売価格データ SRP は、復号後にスタックメモリ 200 に記憶された図 4 B に示すキーファイル KF の権利書データ 106 内に格納されている。

課金処理部 187 による課金処理は、利用監視部 186 の監視の下、権利書データ 106 が示す使用許諾条件などの権利内容および利用制御状態データ 166 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

また、課金処理部 187 は、操作信号 S165 に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態 (UCS: Usage Control Status) データ 166 を生成し、これをスタックメモリ 200 に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ 166 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 166 には、コンテンツの ID、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれた SAM の SAM_ID、購入を行なったユーザの USER_ID などが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁ からコンテンツプロバイダ 101 に利用制御状態データ 166 をコンテンツデータ C の購入と同時にリアルタイムに送信し、コンテンツプロバイダ 101 が EMD サービスセンタ 102 に、利用履歴データ 108 を所定の期間内に SAM105₁ に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ 166 が、コンテンツプロバイダ 101 および EMD サービスセンタ 102 の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ 166 をコンテンツプロバイダ 101 にリアルタイムに送信する。

EMD サービスセンタ管理部 185 は、外部メモリ管理部 811 を介して外部メモリ 201 から読み出した利用履歴データ 108 を EMD サービスセンタ 102 に送信する。

このとき、EMD サービスセンタ管理部 185 は、署名処理部 189 において、秘密鍵データ $K_{SAM1,s}$ を用いて利用履歴データ 108 の署名データ $SIG_{200,sam1}$ を作成し、署名データ $SIG_{200,sam1}$ を利用履歴データ 108 と共に EMD サービスセンタ 102 に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

ダウンロードメモリ管理部182は、例えば、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

以下、SAM105、内での処理の流れについて説明する。

先ず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図23および図24を参照しながら説明する。

図24は、当該処理のフローチャートである。

ステップSH1：課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSH2の処理が行われ、そうでない場合にはステップSH3の処理が行われる。

ステップSH2：課金処理部187によって、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図16に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図16に示す復号部221において復号された後に、復号部222に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データ K_c および半開示パラメータデータ199が、図16に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データ K_c および半開示パラメータデータ199に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データ K_c を用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長

された後に、電子透かし情報処理部 2 2 4 に出力される。

次に、電子透かし情報処理部 2 2 4 においてユーザ電子透かし情報用データ 1 8 6 がコンテンツデータ C に埋め込まれた後、コンテンツデータ C が再生モジュール 1 6 9 において再生され、コンテンツデータ C に応じた音響が出力される。

ステップ S H 3 : ユーザが購入・利用形態決定操作部 1 6 5 を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号 S 1 6 5 が課金処理部 1 8 7 に出力される。

ステップ S H 4 : 課金処理部 1 8 7 において、決定された購入形態に応じた利用履歴データ 1 0 8 および利用制御状態データ 1 6 6 が生成され、利用履歴データ 1 0 8 が外部メモリ管理部 8 1 1 を介して外部メモリ 2 0 1 に書き込まれると共に、利用制御状態データ 1 6 6 がスタックメモリ 2 0 0 に書き込まれる。

以後は、利用監視部 1 8 6 において、利用制御状態データ 1 6 6 によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

ステップ S H 5 : スタックメモリ 2 0 0 に格納されているキーファイル K F に、利用制御状態データ 1 6 6 が加えられ、購入形態が決定した後述する図 2 9 B に示す新たなキーファイル K F₁ が生成される。キーファイル K F₁ は、スタックメモリ 2 0 0 に記憶される。

図 2 9 B に示すように、キーファイル K F₁ に格納された利用制御状態データ 1 6 6 はストレージ鍵データ K_{STR} を用いて D E S の C B C モードを利用して暗号化されている。また、当該ストレージ鍵データ K_{STR} を M A C 鍵データとして用いて生成した M A C 値である M A C_{s00} が付されている。また、利用制御状態データ 1 6 6 および M A C_{s00} からなるモジュールは、メディア鍵データ K_{MBD} を用いて D E S の C B C モードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ K_{MBD} を M A C 鍵データとして用いて生成した M A C 値である M A C_{s01} が付されている。

以下、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図23および図25を参照しながら説明する。

図25は、当該処理のフローチャートである。

ステップS11：課金処理部187が、ユーザによる操作に応じて、再生を行うコンテンツを指定した操作信号S165を入力する。

ステップS12：課金処理部187は、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが読み出される。

ステップS13：当該読み出されたコンテンツファイルCFが図16に示す復号・伸長モジュール163に出力される。このとき、図23に示す相互認証部170と、図16に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

ステップS14：復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

ステップS15：課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。

利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG_{200, SAM1}と共にEMDサービスセンタ102に送信される。

以下、図26に示すように、例えば、ネットワーク機器160₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファ

イルCFおよびキーファイルKFを、バス191を介して、AV機器160₂のSAM105₂に転送する場合のSAM105₁内での処理の流れを図27および図28を参照しながら説明する。

図28は、当該処理のフローチャートである。

ステップSJ1：ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器160₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部187に出力される。

これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ201に記憶されている利用履歴データ108を更新する。

ステップSJ2：ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図29Aに示すコンテンツファイルCFをSAM管理部190に出力する。

ステップSJ3：スタックメモリ200から読み出した図29Bに示すキーファイルKF₁を、署名処理部189およびSAM管理部190に出力する。

ステップSJ4：署名処理部189は、スタックメモリ200から読み出したキーファイルKF₁の署名データSIG_{42, SAM1}を作成し、これをSAM管理部190に出力する。

また、SAM管理部190は、記憶部192から、図29Cに示す公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22, BSC}を読み出す。

ステップSJ5：相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。

SAM管理部190は、図29A、図29B、図29Cに示すデータからなる新たなセキュアコンテナを作成する。

ステップSJ6：暗号化・復号部171において、セッション鍵データK_{SES}を用いて暗号化した後に、図26に示すAV機器160₂のSAM105₂に出

力する。

このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

以下、図26に示すように、SAM105₁から入力したコンテンツファイルCFなどを、RAM型などの記録媒体（メディア）に書き込む際のSAM105₂内での処理の流れを、図30および図31を参照しながら説明する。

図31は、当該処理のフローチャートである。

ステップSK1：SAM105₂のSAM管理部190は、図26に示すように、図29Aに示すコンテンツファイルCFと、図29Bに示すキーファイルKF₁およびその署名データSIG_{42, SAM1}と、図29Cに示す公開鍵署名データCER_{SAM1}およびその署名データSIG_{22, BSC}とを、ネットワーク機器160₁のSAM105₁から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF₁およびその署名データSIG_{42, SAM1}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22, BSC}とが、相互認証部170とSAM105₁の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

次に、セッション鍵データK_{SES}を用いて復号されたキーファイルKF₁およびその署名データSIG_{42, SAM1}と、公開鍵署名データCER_{SAM1}およびその署名データSIG_{22, BSC}とが、スタックメモリ200に書き込まれる。

ステップSK2：署名処理部189は、スタックメモリ200から読み出した署名データSIG_{22, BSC}を、記憶部192から読み出した公開鍵データK_{BSC, P}を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1, P}を用いて、署名データSIG_{42, SAM1}の正当を確認する。

次に、署名データ $SIG_{42, SAM1}$ の正当性、すなわちキーファイル KF_1 の作成者の正当性が確認されると、図 29B に示すキーファイル KF_1 をスタックメモリ 200 から読み出して暗号化・復号部 173 に出力する。

なお、当該例では、キーファイル KF_1 の作成者と送信元とが同じ場合を述べたが、キーファイル KF_1 の作成者と送信元とが異なる場合には、キーファイル KF_1 に対して作成者の署名データと送信者と署名データとが作成され、署名処理部 189 において、双方の署名データの正当性が検証される。

ステップ SK3: 暗号化・復号部 173 は、記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いてキーファイル KF_1 を順に暗号化してメディア SAM 管理部 197 に出力する。

なお、メディア鍵データ K_{MED} は、図 27 に示す相互認証部 170 と図 26 に示す RAM 型の記録媒体 250 のメディア SAM 252 との間の相互認証によって記憶部 192 に事前に記憶されている。

ここで、記録用鍵データ K_{STR} は、例えば SACD (Super Audio Compact Disc)、DVD (Digital Versatile Disc) 機器、CD-R 機器および MD (Mini Disc) 機器などの種類 (当該例では、AV 機器 160₂) に応じて決まるデータであり、機器の種類と記録媒体の種類とを 1 対 1 で対応づけるために用いられる。なお、SACD と DVD とでは、ディスク媒体の物理的な構造が同じであるため、DVD 機器を用いて SACD の記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ K_{STR} は、このような場合において、不正コピーを防止する役割を果たす。

また、メディア鍵データ K_{MED} は、記録媒体 (当該例では、RAM 型の記録媒体 250) にユニークなデータである。

メディア鍵データ K_{MED} は、記録媒体 (当該例では、図 26 に示す RAM 型の記録媒体 250) 側に格納されており、記録媒体のメディア SAM においてメデ

ィア鍵データ K_{MBD} を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ K_{MBD} は、記録媒体にメディア SAM が搭載されている場合には、当該メディア SAM 内に記憶されており、記録媒体にメディア SAM が搭載されていない場合には、例えば、RAM 領域内のホスト CPU 810 の管理外の領域に記憶されている。

なお、本実施形態のように、機器側の SAM（当該例では、SAM105₂）とメディア SAM（当該例では、メディア SAM252）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データ K_{MBD} を機器側の SAM に転送し、機器側の SAM においてメディア鍵データ K_{MBD} を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データ K_{STR} およびメディア鍵データ K_{MBD} が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

また、購入者鍵データ K_{PIN} は、コンテンツファイル CF の購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対して EMD サービスセンタ 102 によって割り当てられる。購入者鍵データ K_{PIN} は、EMD サービスセンタ 102 において管理される。

ステップ SK4：メディア SAM 管理部 197 は、SAM 管理部 190 から入力したコンテンツファイル CF および暗号化・復号部 173 から入力したキーファイル KF_1 を、図 26 に示す記録モジュール 260 に出力する。

そして、記録モジュール 260 は、メディア SAM 管理部 197 から入力したコンテンツファイル CF およびキーファイル KF_1 を、図 26 に示す RAM 型の記録媒体 250 の RAM 領域 251 に書き込む。この場合に、キーファイル KF_1 を、メディア SAM 252 内に書き込むようにしてもよい。

以下、コンテンツの購入形態が未決定の図 6 に示す ROM 型の記録媒体 130 をユーザホームネットワーク 303 がオフラインで配給を受けた場合に、AV 機器 160₂ において購入形態を決定する際の処理の流れを図 32、図 33、図 3

4、図35を参照しながら説明する。

ステップSL1：AV機器160₂のSAM105₂は、先ず、図33に示す相互認証部170と図6に示すROM型の記録媒体130のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データK_{MED}を入力する。

なお、SAM105₂が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。

ステップSL2：ROM型の記録媒体130のRAM領域132に記録されているセキュアコンテナ104に格納された図4B、Cに示すキーファイルKFおよびその署名データSIG_{7, CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1, BSC}とが、メディアSAM管理部197を介して入力され、これらがスタックメモリ200に書き込まれる。

ステップSL3：署名処理部189において、署名データSIG_{1, BSC}の正当性を確認した後に、公開鍵証明書データCER_{CP}から公開鍵データK_{CP, P}を取り出し、この公開鍵データK_{CP, P}を用いて、署名データSIG_{7, CP}の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

ステップSL4：署名処理部189において署名データSIG_{7, CP}の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

そして、セキュアコンテナ復号部183において、対応する期間の配信用鍵データKD₁～KD₉を用いて、キーファイルKFを復号する。

ステップSL5：署名処理部189において、公開鍵データK_{BSC, P}を用いて、キーファイルKFに格納された署名データSIG_{1, BSCM}の正当性を確認した後に、キーファイルKF内の公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP, P}を用いて、署名データSIG_{2, CP}～SIG_{4, CP}の正当性、すなわちコンテンツデータC、コンテンツ鍵データK_Cおよび権利書データ106の作成者の

正当性を検証する。

ステップS L 6：課金処理部1 8 7において、ユーザによる図1 6に示す購入・利用形態決定操作部1 6 5の操作によって、試聴モードを示す操作信号S 1 6 5が発生したか否かが判断され、発生したと判断された場合にはステップS L 7の処理が行われ、そうでない場合にはステップS L 8の処理が行われる。

ステップS L 7：図3 3に示す相互認証部1 7 0と図3 2に示す復号・伸長モジュール1 6 3との間で相互認証を行った後に、S A M 1 0 5₂の復号・伸長モジュール管理部1 8 4は、スタックメモリ2 0 0に記憶されているコンテンツ鍵データK cおよび権利書データ1 0 6に格納された半開示パラメータデータ1 9 9、並びにR O M型の記録媒体1 3 0のR O M領域1 3 1から読み出したコンテンツデータCを図3 2に示す復号・伸長モジュール1 6 3に出力する。次に、復号・伸長モジュール1 6 3において、コンテンツデータCがコンテンツ鍵データK cを用いて半開示モードで復号された後に伸長され、再生モジュール2 7 0に出力される。そして、再生モジュール2 7 0において、復号・伸長モジュール1 6 3からのコンテンツデータCが試聴モードで再生される。

ステップS L 8：ユーザによる図3 2に示す購入形態決定操作部1 6 5の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号S 1 6 5が課金処理部1 8 7に入力される。

ステップS L 9：課金処理部1 8 7は、操作信号S 1 6 5に応じた利用制御状態データ1 6 6を作成し、これをスタックメモリ2 0 0に書き込む。

また、課金処理部1 8 7は、利用履歴データ1 0 8を作成あるいは更新する。

ステップS L 1 0：スタックメモリ2 0 0から暗号化・復号部1 7 3に、例えば、図4 Bに示すキーファイルK Fに利用制御状態データ1 6 6を格納した図2 9 Bに示す新たなキーファイルK F₁が出力される。

ステップS L 1 1：暗号化・復号部1 7 3は、スタックメモリ2 0 0から読み

出した図 2 9 B に示すキーファイル KF_1 を、記憶部 1 9 2 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MBD} および購入者鍵データ K_{PIN} を用いて順次に暗号化してメディア SAM 管理部 1 9 7 に出力する。

ステップ SL 1 2：図 3 3 に示す相互認証部 1 7 0 と図 3 2 に示すメディア SAM 1 3 3 との間で相互認証を行った後に、SAM 管理部 1 9 7 は、暗号化・復号部 1 7 3 から入力したキーファイル KF_1 を図 3 2 に示す記録モジュール 2 7 1 を介して ROM 型の記録媒体 1 3 0 の RAM 領域 1 3 2 あるいはメディア SAM 1 3 3 内に書き込む。

これにより、購入形態が決定された ROM 型の記録媒体 1 3 0 が得られる。

このとき、課金処理部 1 8 7 が生成した利用制御状態データ 1 6 6 および利用履歴データ 1 0 8 は、所定のタイミングで、スタックメモリ 2 0 0 および外部メモリ 2 0 1 からそれぞれ読み出しされた EMD サービスセンタ 1 0 2 に送信される。

以下、図 3 6 に示すように、AV 機器 1 6 0₁ において購入形態が未決定の ROM 型の記録媒体 1 3 0 からセキュアコンテナ 1 0 4 を読み出して AV 機器 1 6 0₂ に転送し、AV 機器 1 6 0₂ において購入形態を決定して RAM 型の記録媒体 2 5 0 に書き込む際の処理の流れを図 3 7 および図 3 8 を用いて説明する。

図 3 7 は、SAM 1 0 5₁ における当該処理のフローチャートである。

図 3 8 は、SAM 1 0 5₂ における当該処理のフローチャートである。なお、ROM 型の記録媒体 1 3 0 から RAM 型の記録媒体 2 5 0 へのセキュアコンテナ 1 0 4 の転送は、図 1 に示すネットワーク機器 1 6 0₁ および AV 機器 1 6 0₁ ~ 1 6 0₄ のいずれの間で行ってもよい。

ステップ SM 1 1（図 3 7）：AV 機器 1 6 0₁ の SAM 1 0 5₁ と ROM 型の記録媒体 1 3 0 のメディア SAM 1 3 3 との間で相互認証を行い、ROM 型の記録媒体 1 3 0 のメディア鍵データ K_{MBD_1} を SAM 1 0 5₁ に転送する。

このとき、同様に、V 機器 1 6 0₂ の SAM 1 0 5₂ と RAM 型の記録媒体 2

50のメディアSAM252との間で相互認証を行い、RAM型の記録媒体250のメディア鍵データ K_{MED2} をSAM105₂に転送する。

ステップSM12: SAM105₂は、RAM領域132から読み出した図4B、CキーファイルKF、署名データ $SIG_{7, CP}$ 、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1, BSC}$ とを、図40に示す暗号化・復号部172において、対応する期間の配信用鍵データ $KD_1 \sim KD_9$ を用いて順に復号する。

次に、暗号化・復号部172で復号されたコンテンツファイルCFは、暗号化・復号部171に出力され、SAM105₂と105₁との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化された後に、SAM管理部190に出力される。

また、暗号化・復号部172で復号されたキーファイルKFは、暗号化・復号部171および署名処理部189に出力される。

ステップSM13: 署名処理部189は、SAM105₂の秘密鍵データ $K_{SAM2, S}$ を用いて、キーファイルKFの署名データ $SIG_{350, SAM2}$ を作成し、これを暗号化・復号部171に出力する。

ステップSM14: 暗号化・復号部171は、記憶部192から読み出したSAM105₂の公開鍵証明書データ CER_{SAM2} およびその署名データ $SIG_{351, BSC}$ と、キーファイルKFおよびその署名データ $SIG_{350, SAM2}$ と、ROM型の記録媒体130のROM領域131から読み出した図4Aに示すコンテンツファイルCFとを、SAM105₂と105₁との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化した後に、SAM管理部190を介して、AV機器160₂のSAM105₂に出力する。

ステップSN1 (図38): SAM105₂では、図41に示すように、SAM管理部190を介してSAM105₂から入力されたコンテンツファイルCFが、暗号化・復号部171においてセッション鍵データ K_{SES} を用いて復号され

た後に、メディアSAM管理部197を介してRAM型の記録媒体250のRAM領域251に書き込まれる。

また、SAM管理部190を介してSAM105_sから入力されたキーファイルKFおよびその署名データSIG_{350, SAMs}と、公開鍵証明書データCER_{SAMs}およびその署名データSIG_{351, BSc}とが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データK_{SBS}を用いて復号される。

ステップSN2：当該復号された署名データSIG_{351, BSc}が、署名処理部189において署名検証され、その正当性が確認されると、公開鍵証明書データCER_{SAMs}に格納された公開鍵データK_{SAMs}を用いて、署名データSIG_{350, SAMs}の正当性、すなわちキーファイルKFの送信元の正当性が確認される。

そして、署名データSIG_{350, SAMs}の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

ステップSN3：セキュアコンテナ復号部183は、対応する期間の配信用鍵データKD₁～KD_sを用いて、キーファイルKFを復号し、所定の署名検証を経た後に、当該復号したキーファイルKFをスタックメモリ200に書き込む。

その後、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。そして、利用監視部186によって、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

ステップSN4：課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSN5の処理が行われ、そうでない場合にはステップSN6の処理が行われる。

ステップSN5：ユーザによって試聴モードが選択されると、既にセッション

鍵データ K_{SBS} で復号されたコンテンツファイル CF のコンテンツデータ C と、スタックメモリ 200 に記憶されたコンテンツ鍵データ K_c 、権利書データ 106 から得られた半開示パラメータデータ 199 およびユーザ電子透かし情報用データ 196 とが、相互認証を経た後に、図 36 に示す復号・伸長モジュール管理部 184 を介して再生モジュール 270 に出力される。そして、再生モジュール 270 において、試聴モードに対応したコンテンツデータ C の再生が行われる。

ステップ SN 6 : ユーザによる図 36 に示す購入・利用形態決定操作部 165 の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号 S165 が、課金処理部 187 に出力される。

ステップ SN 7 : 課金処理部 187 において、決定された購入・利用形態に応じて利用制御状態データ 166 および利用履歴データ 108 が生成され、これがスタックメモリ 200 および外部メモリ 201 にそれぞれ書き込まれる。

ステップ SN 8 : スタックメモリ 200 から読み出された利用制御状態データ 166 を格納した例えば図 29B に示すキーファイル KF_1 が作成され、これが暗号化・復号部 173 に出力される。

ステップ SN 9 : 暗号化・復号部 173 において記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED2} および購入者鍵データ K_{PIN} を用いて順に暗号化され、メディア SAM 管理部 197 に出力される。

ステップ SN 10 : メディア SAM 管理部 197 によって、キーファイル KF_1 が、図 36 に示す記録モジュール 271 によって RAM 型の記録媒体 250 の RAM 領域 251 あるいはメディア SAM 252 に書き込まれる。

また、利用制御状態データ 166 および利用履歴データ 108 は、所定のタイミングで、EMD サービスセンタ 102 に送信される。

以下、SAM105₁ ~ 105₄ の実現方法について説明する。

SAM105₁ ~ 105₄ の機能をハードウェアとして実現する場合は、メモリを内蔵した ASIC 型の CPU を用いて、そのメモリには、図 17 に示す各機

能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

例えば、図 17 に示す暗号化・復号部 171 などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部 171 をソフトウェアとして実装してもよい。

また、図 17 に示す記憶部 192 や、図 17 に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁～105₄に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。

また、SAM105₁～105₄には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

上述したように、SAM105₁～105₄は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105₁～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側

のメモリー空間を管理するMMU(Memory Magagement Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM105₁～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM105₁～105₄自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

SAM105₁～105₄の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（MiniOS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

次に、図16に示す復号・伸長モジュール163について説明する。

図16に示すように、復号・伸長モジュール163は、相互認証部220、復

号部 2 2 1、復号部 2 2 2、伸長部 2 2 3、電子透かし情報処理部 2 2 4 および半開示処理部 2 2 5 を有する。

相互認証部 2 2 0 は、復号・伸長モジュール 1 6 3 が SAM 1 0 5₁ からデータを入力する際に、図 2 6 に示す相互認証部 1 7 0 との間で相互認証を行ってセッション鍵データ K_{SES} を生成する。

復号部 2 2 1 は、SAM 1 0 5₁ から入力したコンテンツ鍵データ K_c 、半開示パラメータデータ 1 9 9、ユーザ電子透かし情報用データ 1 9 6 およびコンテンツデータ C を、セッション鍵データ K_{SES} を用いて復号する。そして、復号部 2 2 1 は、復号したコンテンツ鍵データ K_c およびコンテンツデータ C を復号部 2 2 2 に出力し、復号したユーザ電子透かし情報用データ 1 9 6 を電子透かし情報処理部 2 2 4 に出力し、半開示パラメータデータ 1 9 9 を半開示処理部 2 2 5 に出力する。

復号部 2 2 2 は、半開示処理部 2 2 5 からの制御に基づいて、コンテンツ鍵データ K_c を用いて、コンテンツデータ C を半開示状態で復号し、復号したコンテンツデータ C を伸長部 2 2 3 に出力する。

伸長部 2 2 3 は、復号されたコンテンツデータ C を伸長して、電子透かし情報処理部 2 2 4 に出力する。

伸長部 2 2 3 は、例えば、図 4 A に示すコンテンツファイル CF に格納された A/V 伸長用ソフトウェアを用いて伸長処理を行い、例えば、 $ATRA C 3$ 方式で伸長処理を行う。

電子透かし情報処理部 2 2 4 は、復号されたユーザ電子透かし情報用データ 1 9 6 に応じたユーザ電子透かし情報を、復号されたコンテンツデータ C に埋め込み、新たなコンテンツデータ C を生成する。電子透かし情報処理部 2 2 4 は、当該新たなコンテンツデータ C を再生モジュール 1 6 9 に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータ C を再生するときに、復号・伸長モジュール 1 6 3 において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。

また、半開示処理部225は、その他に、半開示パラメータデータ199に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

再生モジュール168は、復号および伸長されたコンテンツデータCに応じた再生を行う。

次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図42Aは、コンテンツプロバイダ101からSAM105₁にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{SSS}で暗号化したモジュールMod₅₀が送信される。

モジュールMod₅₀には、モジュールMod₅₁およびその秘密鍵データK_{CP, S}による署名データSIG_{CP}が格納されている。

モジュールMod₅₁には、コンテンツプロバイダ101の秘密鍵データK_{CP, P}を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}対しての秘密鍵データK_{BSC, S}による署名データSIG_{BSC}と、送信するデータDataとが格納されている。

このように、公開鍵証明書データ CER_{CP} を格納したモジュール Mod_{50} を、コンテンツプロバイダ 101 から $SAM105_1$ に送信することで、 $SAM105_1$ において署名データ SIG_{CP} の検証を行なう際に、EMDサービスセンタ 102 から $SAM105_1$ に公開鍵証明書データ CER_{CP} を送信する必要がなくなる。

図 4 2 B、図 4 2 C は、コンテンツプロバイダ 101 から $SAM105_1$ にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ 101 から $SAM105_1$ に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 4 2 B に示すモジュール Mod_{52} が送信される。

モジュール Mod_{52} には、送信するデータ $Data$ と、その秘密鍵データ $K_{CP,s}$ による署名データ SIG_{CP} とが格納されている。

また、EMDサービスセンタ 102 から $SAM105_1$ には、EMDサービスセンタ 102 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 4 2 C に示すモジュール Mod_{53} が送信される。

モジュール Mod_{53} には、コンテンツプロバイダ 101 の公開鍵証明書データ CER_{CP} と、その秘密鍵データ $K_{BSC,s}$ による署名データ SIG_{BSC} とが格納されている。

図 4 2 D は、 $SAM105_1$ からコンテンツプロバイダ 101 にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ 101 に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{54} が送信される。

モジュール Mod_{54} には、モジュール Mod_{53} およびその秘密鍵データ K_{SAM1}

、 s による署名データ SIG_{SAM1} が格納されている。

モジュール Mod_{55} には、 $SAM105_1$ の秘密鍵データ $K_{SAM1, P}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC, s}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

このように、公開鍵証明書データ CER_{SAM1} を格納したモジュール Mod_{55} を、 $SAM105_1$ からコンテンツプロバイダ 101 に送信することで、コンテンツプロバイダ 101 において署名データ SIG_{SAM1} の検証を行なう際に、EMD サービスセンタ 102 からコンテンツプロバイダ 101 に公開鍵証明書データ CER_{SAM1} を送信する必要がなくなる。

図 4 2 E、図 4 2 F は、 $SAM105_1$ からコンテンツプロバイダ 101 にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ 101 に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SBS} で暗号化した図 4 2 E に示すモジュール Mod_{58} が送信される。

モジュール Mod_{58} には、送信するデータ $Data$ と、その秘密鍵データ $K_{SAM1, s}$ による署名データ SIG_{SAM1} とが格納されている。

また、EMD サービスセンタ 102 からコンテンツプロバイダ 101 には、EMD サービスセンタ 102 とコンテンツプロバイダ 101 との間の相互認証によって得たセッション鍵データ K_{SBS} で暗号化した図 4 2 F に示すモジュール Mod_{57} が送信される。

モジュール Mod_{57} には、 $SAM105_1$ の公開鍵証明書データ CER_{SAM1} と、その秘密鍵データ $K_{ESC, s}$ による署名データ SIG_{ESC} とが格納されている。

図 4 3 A は、コンテンツプロバイダ 101 から EMD サービスセンタ 102 にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明

するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{58} が送信される。

モジュール Mod_{58} には、モジュール Mod_{58} およびその秘密鍵データ $K_{CP, S}$ による署名データ SIG_{CP} が格納されている。

モジュール Mod_{58} には、コンテンツプロバイダ101の秘密鍵データ $K_{CP, P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対する秘密鍵データ $K_{BSC, S}$ による署名データ SIG_{BSC} と、送信するデータ $Data$ とが格納されている。

図43Bは、コンテンツプロバイダ101からEMDサービスセンタ102にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図43Bに示すモジュール Mod_{58} が送信される。

モジュール Mod_{58} には、送信するデータ $Data$ と、その秘密鍵データ $K_{CP, S}$ による署名データ SIG_{CP} とが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データ CER_{CP} は既に登録されている。

図43Cは、SAM105₁からEMDサービスセンタ102にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からEMDサービスセンタ102に、EMDサ

ービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データ K_{SBS} で暗号化したモジュール Mod_{81} が送信される。

モジュール Mod_{81} には、モジュール Mod_{82} およびその秘密鍵データ $K_{SAM1,s}$ による署名データ SIG_{SAM1} が格納されている。

モジュール Mod_{82} には、SAM105₁の秘密鍵データ $K_{SAM1,p}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC,s}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

図43Dは、SAM105₁からEMDサービスセンタ102にデータ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁との間の相互認証によって得たセッション鍵データ K_{SBS} で暗号化した図43Dに示すモジュール Mod_{83} が送信される。

モジュール Mod_{83} には、送信するデータ $Data$ と、その秘密鍵データ $K_{SAM1,s}$ による署名データ SIG_{SAM1} とが格納されている。

このとき、EMDサービスセンタ102にはSAM105₁の公開鍵証明書データ CER_{SAM1} は既に登録されている。

以下、SAM105₁～105₄の出荷時におけるEMDサービスセンタ102への登録処理について説明する。

なお、SAM105₁～105₄の登録処理は同じであるため、以下、SAM105₁の登録処理について述べる。

SAM105₁の出荷時には、図11に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部148を介して、図17などに示す記憶部192に以下に示す鍵データが初期登録される。

また、SAM105₁には、例えば、出荷時に、記憶部192などに、SAM

105₁がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部192には、例えば、図21において左側に「*」が付されているSAM105₁の識別子SAM_ID、記録用鍵データK_{STR}、ルート認証局2の公開鍵データK_{R-CA}、EMDサービスセンタ102の公開鍵データK_{BSC, P}、SAM105₁の秘密鍵データK_{SAM1, S}、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22, BSC}、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データCER_{SAM1}は、SAM105₁を出荷後に登録する際にEMDサービスセンタ102からSAM105₁に送信してもよい。

ここで、ルート認証局2の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているRSAを使用し、データ長は例えば1024ビットである。公開鍵データK_{R-CA}は、図1に示すルート認証局2によって発行される。

また、EMDサービスセンタ102の公開鍵データK_{BSC, P}は、短いデータ長でRSAと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば160ビットである。但し、暗号化の強度を考慮すると、公開鍵データK_{BSC, P}は192ビット以上であることが望ましい。また、EMDサービスセンタ102は、ルート認証局92に公開鍵データK_{BSC, P}を登録する。

また、ルート認証局92は、公開鍵データK_{BSC, P}の公開鍵証明書データCER_{BSC}を作成する。公開鍵データK_{BSC, P}を格納した公開鍵証明書データCER_{BSC}は、好ましく、SAM105₁の出荷時に記憶部192に記憶される。この場合に、公開鍵証明書データCER_{BSC}は、ルート認証局92の秘密鍵データK_{ROOT, S}で署名されている。

EMDサービスセンタ102は、乱数を発生してSAM105₁の秘密鍵デー

タ $K_{SAM1, S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1, P}$ を生成する。

また、EMDサービスセンタ102は、ルート認証局92の認証をもらって、公開鍵データ $K_{SAM1, P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{ESC, S}$ を用いて署名データを添付する。すなわち、EMDサービスセンタ102は、セカンドCA（認証局）として機能を果たす。

また、 $SAM105_1$ には、図11に示すEMDサービスセンタ102のSAM管理部149により、EMDサービスセンタ102の管理下にある一意（ユニーク）な識別子 SAM_ID が割り当てられ、これが $SAM105_1$ の記憶部192に格納されると共に、図11に示すSAMデータベース149aにも格納され、EMDサービスセンタ102によって管理される。

また、 $SAM105_1$ は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データ $KD_1 \sim KD_n$ が転送される。

すなわち、 $SAM105_1$ を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録が必要である。この登録手続は、例えば、 $SAM105_1$ を搭載している機器（当該例では、ネットワーク機器160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

$SAM105_1$ は、上述した登録手続を経た後でないと使用できない。

EMDサービスセンタ102は、 $SAM105_1$ のユーザによる登録手続に応じて、ユーザに固有の識別子 $USER_ID$ を発行し、例えば、図11に示すSAMデータベース149aにおいて、 SAM_ID と $USER_ID$ との対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、 $SAM105_1$ のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサ

ービスセンタ 102 に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMD サービスセンタ 102 は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

次に、図 21 に示すように、SAM 105₁ 内の記憶部 192 に SAM 登録リストを格納する手順について説明する。

図 1 に示す SAM 105₁ は、例えば、バス 191 として IEEE 1394 シリアルバスを用いた場合に、バス 191 に接続された機器の電源を立ち上げたり、新しい機器をバス 191 に接続したときに生成されるトポロジーマップを利用して、自分の系に存在する SAM 105₂ ～ SAM 105₄ の SAM 登録リストを得る。

なお、IEEE 1394 シリアルバスであるバス 191 に応じて生成されたトポロジーマップは、例えば、図 44 に示すように、バス 191 に SAM 105₁ ～ 105₄ に加えて AV 機器 160₅、160₆ の SCMS 処理回路 105₅、105₆ が接続されている場合に、SAM 105₁ ～ 105₄ および SCMS 処理回路 105₅、105₆ を対象として生成される。

従って、SAM 105₁ は、当該トポロジーマップから、SAM 105₁ ～ 105₄ についての情報を抽出して SAM 登録リストを生成する。

SAM 登録リストのデータフォーマットは、例えば、図 45 に示される。

そして、SAM 105₁ は、当該 SAM 登録リストを、EMD サービスセンタ 102 に登録して署名を得る。

これらの処理は、バス 191 のセッションを利用して SAM 105₁ が自動的に行い、EMD サービスセンタ 102 に SAM 登録リストの登録命令を発行する。

EMD サービスセンタ 102 は、SAM 105₁ から図 45 に示す SAM 登録リストを受けると、有効期限を確認する。そして、EMD サービスセンタ 102

は、登録時にSAM105₁より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。

また、EMDサービスセンタ102は、決済時にはSAM105₁に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。

なお、SAMリボケーションリストは、同一系の（同一のバス191に接続されている）SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。

図46は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1：EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データK_{CP}、Pの公開鍵証明書CER_{CP}をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、SAM105₁～105₄が所定の登録処理を経た後に、SAM105₁～105₄の公開鍵データK_{SAM1, P}～K_{SAM4, P}の公開鍵証明書CER_{CP1}～CER_{CP4}をSAM105₁～105₄に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の6カ月分の配信用鍵データKD₁～KD₆をコンテンツプロバイダ101に送信し、3カ月分の配信用鍵データKD₁～KD₃をユーザホームネットワーク103に送信する。

このように、EMDシステム100では、配信用鍵データKD₁～KD₆を予

めSAM105₁～105₄に配給しているため、SAM105₁～105₄とEMDサービスセンタ102との間がオフラインの状態でも、SAM105₁～105₄においてコンテンツプロバイダ101から配給されたセキュアコンテナ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM105₁～105₄とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、SAM105₁～105₄からEMDサービスセンタ102に送信される。

ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図7Aに示す権利登録要求モジュールMod₂を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データK_cを登録して権威化する。

ステップS3：コンテンツプロバイダ101は、対応する期間の配信用鍵データKD₁～KD₈などを用いて暗号化を行って、図4A、Bに示すコンテンツファイルCFおよびキーファイルKFを作成し、これらと図4Cに示す公開鍵証明書データCER₁とを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103に配給する。

ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、セキュアコンテナ104を対応する期間の配信用鍵データKD₁～KD₈などを用いて復号し、セキュアコンテナ104の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテナ104が正当なコン

コンテンツプロバイダ 101 から送信されたか否かを確認する。

ステップ S5 : SAM105₁ ~ SAM105₄ において、ユーザによる図 16 に示す購入・利用形態決定操作部 165 の操作に応じた操作信号 S165 に基づいて、購入・利用形態を決定する。

このとき、図 23 に示す利用監視部 186 において、セキュアコンテナ 104 に格納された権利書データ 106 に基づいて、ユーザによるコンテンツファイル CF の購入・利用形態が管理される。

ステップ S6 : SAM105₁ ~ SAM105₄ の図 23 に示す課金処理部 187 において、操作信号 S165 に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ 108 および利用制御状態データ 166 が生成し、これらを EMD サービスセンタ 102 に送信する。

ステップ S7 : EMD サービスセンタ 102 は、図 11 に示す決算処理部 142 において、利用履歴データ 108 に基づいて決済処理を行い、決済請求権データ 152 および決済レポートデータ 107 を作成する。EMD サービスセンタ 102 は、決済請求権データ 152 およびその署名データ SIG_{ss} を、図 1 に示すペイメントゲートウェイ 90 を介して、決済機関 91 に送信する。また、EMD サービスセンタ 102 は、決済レポートデータ 107 をコンテンツプロバイダ 101 に送信する。

ステップ S8 : 決済機関 91 において、署名データ SIG_{ss} の検証を行った後に、決済請求権データ 152 に基づいて、ユーザが支払った金額が、コンテンツプロバイダ 101 の所有者に分配される。

以上説明したように、EMD システム 100 では、図 4 に示すフォーマットのセキュアコンテナ 104 をコンテンツプロバイダ 101 からユーザホームネットワーク 103 に配給し、セキュアコンテナ 104 内のキーファイル KF についての処理を SAM105₁ ~ 105₄ 内で行う。

また、キーファイル KF に格納されたコンテンツ鍵データ Kc および権利書デ

ータ106は、配信鍵データKD₁～KD₅を用いて暗号化されており、配信鍵データKD₁～KD₅を保持しているSAM105₁～105₅内でのみ復号される。そして、SAM105₁～105₅では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁～105₅におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂～160₅においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

第1実施形態の第1変形例

上述した実施形態では、図4Bに示すように、コンテンツプロバイダ101において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁～105₅において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁～105₅にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい。

このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

また、上述した実施形態では、図4Bに示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データK_{sp}を用いて作成した署名データを添付する。

第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図47に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105_nに、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a, 101b, 101c, 101d, 101e, 101f, 101g, 101h, 101i, 101j, 101k, 101l, 101m, 101n, 101o, 101p, 101q, 101r, 101s, 101t, 101u, 101v, 101w, 101x, 101y, 101z, 101aa, 101ab, 101ac, 101ad, 101ae, 101af, 101ag, 101ah, 101ai, 101aj, 101ak, 101al, 101am, 101an, 101ao, 101ap, 101aq, 101ar, 101as, 101at, 101au, 101av, 101aw, 101ax, 101ay, 101az, 101ba, 101bb, 101bc, 101bd, 101be, 101bf, 101bg, 101bh, 101bi, 101bj, 101bk, 101bl, 101bm, 101bn, 101bo, 101bp, 101bq, 101br, 101bs, 101bt, 101bu, 101bv, 101bw, 101bx, 101by, 101bz, 101ca, 101cb, 101cc, 101cd, 101ce, 101cf, 101cg, 101ch, 101ci, 101cj, 101ck, 101cl, 101cm, 101cn, 101co, 101cp, 101cq, 101cr, 101cs, 101ct, 101cu, 101cv, 101cw, 101cx, 101cy, 101cz, 101da, 101db, 101dc, 101dd, 101de, 101df, 101dg, 101dh, 101di, 101dj, 101dk, 101dl, 101dm, 101dn, 101do, 101dp, 101dq, 101dr, 101ds, 101dt, 101du, 101dv, 101dw, 101dx, 101dy, 101dz, 101ea, 101eb, 101ec, 101ed, 101ee, 101ef, 101eg, 101eh, 101ei, 101ej, 101ek, 101el, 101em, 101en, 101eo, 101ep, 101eq, 101er, 101es, 101et, 101eu, 101ev, 101ew, 101ex, 101ey, 101ez, 101fa, 101fb, 101fc, 101fd, 101fe, 101ff, 101fg, 101fh, 101fi, 101fj, 101fk, 101fl, 101fm, 101fn, 101fo, 101fp, 101fq, 101fr, 101fs, 101ft, 101fu, 101fv, 101fw, 101fx, 101fy, 101fz, 101ga, 101gb, 101gc, 101gd, 101ge, 101gf, 101gg, 101gh, 101gi, 101gj, 101gk, 101gl, 101gm, 101gn, 101go, 101gp, 101gq, 101gr, 101gs, 101gt, 101gu, 101gv, 101gw, 101gx, 101gy, 101gz, 101ha, 101hb, 101hc, 101hd, 101he, 101hf, 101hg, 101hh, 101hi, 101hj, 101hk, 101hl, 101hm, 101hn, 101ho, 101hp, 101hq, 101hr, 101hs, 101ht, 101hu, 101hv, 101hw, 101hx, 101hy, 101hz, 101ia, 101ib, 101ic, 101id, 101ie, 101if, 101ig, 101ih, 101ii, 101ij, 101ik, 101il, 101im, 101in, 101io, 101ip, 101iq, 101ir, 101is, 101it, 101iu, 101iv, 101iw, 101ix, 101iy, 101iz, 101ja, 101jb, 101jc, 101jd, 101je, 101jf, 101jg, 101jh, 101ji, 101jj, 101jk, 101jl, 101jm, 101jn, 101jo, 101jp, 101jq, 101jr, 101js, 101jt, 101ju, 101jv, 101jw, 101jx, 101jy, 101jz, 101ka, 101kb, 101kc, 101kd, 101ke, 101kf, 101kg, 101kh, 101ki, 101kj, 101kk, 101kl, 101km, 101kn, 101ko, 101kp, 101kq, 101kr, 101ks, 101kt, 101ku, 101kv, 101kw, 101kx, 101ky, 101kz, 101la, 101lb, 101lc, 101ld, 101le, 101lf, 101lg, 101lh, 101li, 101lj, 101lk, 101ll, 101lm, 101ln, 101lo, 101lp, 101lq, 101lr, 101ls, 101lt, 101lu, 101lv, 101lw, 101lx, 101ly, 101lz, 101ma, 101mb, 101mc, 101md, 101me, 101mf, 101mg, 101mh, 101mi, 101mj, 101mk, 101ml, 101mm, 101mn, 101mo, 101mp, 101mq, 101mr, 101ms, 101mt, 101mu, 101mv, 101mw, 101mx, 101my, 101mz, 101na, 101nb, 101nc, 101nd, 101ne, 101nf, 101ng, 101nh, 101ni, 101nj, 101nk, 101nl, 101nm, 101nn, 101no, 101np, 101nq, 101nr, 101ns, 101nt, 101nu, 101nv, 101nw, 101nx, 101ny, 101nz, 101oa, 101ob, 101oc, 101od, 101oe, 101of, 101og, 101oh, 101oi, 101oj, 101ok, 101ol, 101om, 101on, 101oo, 101op, 101oq, 101or, 101os, 101ot, 101ou, 101ov, 101ow, 101ox, 101oy, 101oz, 101pa, 101pb, 101pc, 101pd, 101pe, 101pf, 101pg, 101ph, 101pi, 101pj, 101pk, 101pl, 101pm, 101pn, 101po, 101pp, 101pq, 101pr, 101ps, 101pt, 101pu, 101pv, 101pw, 101px, 101py, 101pz, 101qa, 101qb, 101qc, 101qd, 101qe, 101qf, 101qg, 101qh, 101qi, 101qj, 101qk, 101ql, 101qm, 101qn, 101qo, 101qp, 101qq, 101qr, 101qs, 101qt, 101qu, 101qv, 101qw, 101qx, 101qy, 101qz, 101ra, 101rb, 101rc, 101rd, 101re, 101rf, 101rg, 101rh, 101ri, 101rj, 101rk, 101rl, 101rm, 101rn, 101ro, 101rp, 101rq, 101rr, 101rs, 101rt, 101ru, 101rv, 101rw, 101rx, 101ry, 101rz, 101sa, 101sb, 101sc, 101sd, 101se, 101sf, 101sg, 101sh, 101si, 101sj, 101sk, 101sl, 101sm, 101sn, 101so, 101sp, 101sq, 101sr, 101ss, 101st, 101su, 101sv, 101sw, 101sx, 101sy, 101sz, 101ta, 101tb, 101tc, 101td, 101te, 101tf, 101tg, 101th, 101ti, 101tj, 101tk, 101tl, 101tm, 101tn, 101to, 101tp, 101tq, 101tr, 101ts, 101tt, 101tu, 101tv, 101tw, 101tx, 101ty, 101tz, 101ua, 101ub, 101uc, 101ud, 101ue, 101uf, 101ug, 101uh, 101ui, 101uj, 101uk, 101ul, 101um, 101un, 101uo, 101up, 101uq, 101ur, 101us, 101ut, 101uu, 101uv, 101uw, 101ux, 101uy, 101uz, 101va, 101vb, 101vc, 101vd, 101ve, 101vf, 101vg, 101vh, 101vi, 101vj, 101vk, 101vl, 101vm, 101vn, 101vo, 101vp, 101vq, 101vr, 101vs, 101vt, 101vu, 101vv, 101vw, 101vx, 101vy, 101vz, 101wa, 101wb, 101wc, 101wd, 101we, 101wf, 101wg, 101wh, 101wi, 101wj, 101wk, 101wl, 101wm, 101wn, 101wo, 101wp, 101wq, 101wr, 101ws, 101wt, 101wu, 101wv, 101ww, 101wx, 101wy, 101wz, 101xa, 101xb, 101xc, 101xd, 101xe, 101xf, 101xg, 101xh, 101xi, 101xj, 101xk, 101xl, 101xm, 101xn, 101xo, 101xp, 101xq, 101xr, 101xs, 101xt, 101xu, 101xv, 101xw, 101xx, 101xy, 101xz, 101ya, 101yb, 101yc, 101yd, 101ye, 101yf, 101yg, 101yh, 101yi, 101yj, 101yk, 101yl, 101ym, 101yn, 101yo, 101yp, 101yq, 101yr, 101ys, 101yt, 101yu, 101yv, 101yw, 101yx, 101yy, 101yz, 101za, 101zb, 101zc, 101zd, 101ze, 101zf, 101zg, 101zh, 101zi, 101zj, 101zk, 101zl, 101zm, 101zn, 101zo, 101zp, 101zq, 101zr, 101zs, 101zt, 101zu, 101zv, 101zw, 101zx, 101zy, 101zz, 102a, 102b, 102c, 102d, 102e, 102f, 102g, 102h, 102i, 102j, 102k, 102l, 102m, 102n, 102o, 102p, 102q, 102r, 102s, 102t, 102u, 102v, 102w, 102x, 102y, 102z, 103a, 103b, 103c, 103d, 103e, 103f, 103g, 103h, 103i, 103j, 103k, 103l, 103m, 103n, 103o, 103p, 103q, 103r, 103s, 103t, 103u, 103v, 103w, 103x, 103y, 103z, 104a, 104b, 104c, 104d, 104e, 104f, 104g, 104h, 104i, 104j, 104k, 104l, 104m, 104n, 104o, 104p, 104q, 104r, 104s, 104t, 104u, 104v, 104w, 104x, 104y, 104z, 105a, 105b, 105c, 105d, 105e, 105f, 105g, 105h, 105i, 105j, 105k, 105l, 105m, 105n, 105o, 105p, 105q, 105r, 105s, 105t, 105u, 105v, 105w, 105x, 105y, 105z, 106a, 106b, 106c, 106d, 106e, 106f, 106g, 106h, 106i, 106j, 106k, 106l, 106m, 106n, 106o, 106p, 106q, 106r, 106s, 106t, 106u, 106v, 106w, 106x, 106y, 106z, 107a, 107b, 107c, 107d, 107e, 107f, 107g, 107h, 107i, 107j, 107k, 107l, 107m, 107n, 107o, 107p, 107q, 107r, 107s, 107t, 107u, 107v, 107w, 107x, 107y, 107z, 108a, 108b, 108c, 108d, 108e, 108f, 108g, 108h, 108i, 108j, 108k, 108l, 108m, 108n, 108o, 108p, 108q, 108r, 108s, 108t, 108u, 108v, 108w, 108x, 108y, 108z, 109a, 109b, 109c, 109d, 109e, 109f, 109g, 109h, 109i, 109j, 109k, 109l, 109m, 109n, 109o, 109p, 109q, 109r, 109s, 109t, 109u, 109v, 109w, 109x, 109y, 109z, 110a, 110b, 110c, 110d, 110e, 110f, 110g, 110h, 110i, 110j, 110k, 110l, 110m, 110n, 110o, 110p, 110q, 110r, 110s, 110t, 110u, 110v, 110w, 110x, 110y, 110z, 111a, 111b, 111c, 111d, 111e, 111f, 111g, 111h, 111i, 111j, 111k, 111l, 111m, 111n, 111o, 111p, 111q, 111r, 111s, 111t, 111u, 111v, 111w, 111x, 111y, 111z, 112a, 112b, 112c, 112d, 112e, 112f, 112g, 112h, 112i, 112j, 112k, 112l, 112m, 112n, 112o, 112p, 112q, 112r, 112s, 112t, 112u, 112v, 112w, 112x, 112y, 112z, 113a, 113b, 113c, 113d, 113e, 113f, 113g, 113h, 113i, 113j, 113k, 113l, 113m, 113n, 113o, 113p, 113q, 113r, 113s, 113t, 113u, 113v, 113w, 113x, 113y, 113z, 114a, 114b, 114c, 114d, 114e, 114f, 114g, 114h, 114i, 114j, 114k, 114l, 114m, 114n, 114o, 114p, 114q, 114r, 114s, 114t, 114u, 114v, 114w, 114x, 114y, 114z, 115a, 115b, 115c, 115d, 115e, 115f, 115g, 115h, 115i, 115j, 115k, 115l, 115m, 115n, 115o, 115p, 115q, 115r, 115s, 115t, 115u, 115v, 115w, 115x, 115y, 115z, 116a, 116b, 116c, 116d, 116e, 116f, 116g, 116h, 116i, 116j, 116k, 116l, 116m, 116n, 116o, 116p, 116q, 116r, 116s, 116t, 116u, 116v, 116w, 116x, 116y, 116z, 117a, 117b, 117c, 117d, 117e, 117f, 117g, 117h, 117i, 117j, 117k, 117l, 117m, 117n, 117o, 117p, 117q, 117r, 117s, 117t, 117u, 117v, 117w, 117x, 117y, 117z, 118a, 118b, 118c, 118d, 118e, 118f, 118g, 118h, 118i, 118j, 118k, 118l, 118m, 118n, 118o, 118p, 118q, 118r, 118s, 118t, 118u, 118v, 118w, 118x, 118y, 118z, 119a, 119b, 119c, 119d, 119e, 119f, 119g, 119h, 119i, 119j, 119k, 119l, 119m, 119n, 119o, 119p, 119q, 119r, 119s, 119t, 119u, 119v, 119w, 119x, 119y, 119z, 120a, 120b, 120c, 120d, 120e, 120f, 120g, 120h, 120i, 120j, 120k, 120l, 120m, 120n, 120o, 120p, 120q, 120r, 120s, 120t, 120u, 120v, 120w, 120x, 120y, 120z, 121a, 121b, 121c, 121d, 121e, 121f, 121g, 121h, 121i, 121j, 121k, 121l, 121m, 121n, 121o, 121p, 121q, 121r, 121s, 121t, 121u, 121v, 121w, 121x, 121y, 121z, 122a, 122b, 122c, 122d, 122e, 122f, 122g, 122h, 122i, 122j, 122k, 122l, 122m, 122n, 122o, 122p, 122q, 122r, 122s, 122t, 122u, 122v, 122w, 122x, 122y, 122z, 123a, 123b, 123c, 123d, 123e, 123f, 123g, 123h, 123i, 123j, 123k, 123l, 123m, 123n, 123o, 123p, 123q, 123r, 123s, 123t, 123u, 123v, 123w, 123x, 123y, 123z, 124a, 124b, 124c, 124d, 124e, 124f, 124g, 124h, 124i, 124j, 124k, 124l, 124m, 124n, 124o, 124p, 124q, 124r, 124s, 124t, 124u, 124v, 124w, 124x, 124y, 124z, 125a, 125b, 125c, 125d, 125e, 125f, 125g, 125h, 125i, 125j, 125k, 125l, 125m, 125n, 125o, 125p, 125q, 125r, 125s, 125t, 125u, 125v, 125w, 125x, 125y, 125z, 126a, 126b, 126c, 126d, 126e, 126f, 126g, 126h, 126i, 126j, 126k, 126l, 126m, 126n, 126o, 126p, 126q, 126r, 126s, 126t, 126u, 126v, 126w, 126x, 126y, 126z, 127a, 127b, 127c, 127d, 127e, 127f, 127g, 127h, 127i, 127j, 127k, 127l, 127m, 127n, 127o, 127p, 127q, 127r, 127s, 127t, 127u, 127v, 127w, 127x, 127y, 127z, 128a, 128b, 128c, 128d, 128e, 128f, 128g, 128h, 128i, 128j, 128k, 128l, 128m, 128n, 128o, 128p, 128q, 128r, 128s, 128t, 128u, 128v, 128w, 128x, 128y, 128z, 129a, 129b, 129c, 129d, 129e, 129f, 129g, 129h, 129i, 129j, 129k, 129l, 129m, 129n, 129o, 129p, 129q, 129r, 129s, 129t, 129u, 129v, 129w, 129x, 129y, 129z, 130a, 130b, 130c, 130d, 130e, 130f, 130g, 130h, 130i, 130j, 130k, 130l, 130m, 130n, 130o, 130p, 130q, 130r, 130s, 130t, 130u, 130v, 130w, 130x, 130y, 130z, 131a, 131b, 131c, 131d, 131e, 131f, 131g, 131h, 131i, 131j, 131k, 131l, 131m, 131n, 131o, 131p, 131q, 131r, 131s, 131t, 131u, 131v, 131w, 131x, 131y, 131z, 132a, 132b, 132c, 132d, 132e, 132f, 132g, 132h, 132i, 132j, 132k, 132l, 132m, 132n, 132o, 132p, 132q, 132r, 132s, 132t, 132u, 132v, 132w, 132x, 132y, 132z, 133a, 133b, 133c, 133d, 133e, 133f, 133g, 133h, 133i, 133j, 133k, 133l, 133m, 133n, 133o, 133p, 133q, 133r, 133s, 133t, 133u, 133v, 133w, 133x, 133y, 133z, 134a, 134b, 134c, 134d, 134e, 134f, 134g, 134h, 134i, 134j, 134k, 134l, 134m, 134n, 134o, 134p, 134q, 134r, 134s, 134t, 134u, 134v, 134w, 134x, 134y, 134z, 135a, 135b, 135c, 135d, 135e, 135f, 135g, 135h, 135i, 135j, 135k, 135l, 135m, 135n, 135o, 135p, 135q, 135r, 135s, 135t, 135u, 135v, 135w, 135x, 135y, 135z, 136a, 136b, 136c, 136d, 136e, 136f, 136g, 136h, 136i, 136j, 136k, 136l, 136m, 136n, 136o, 136p, 136q, 136r, 136s, 136t, 136u, 136v, 136w, 136x, 136y, 136z, 137a, 137b, 137c, 137d, 137e, 137f, 137g, 137h, 137i, 137j, 137k, 137l, 137m, 137n, 137o, 137p, 137q, 137r, 137s, 137t, 137u, 137v, 137w, 137x, 137y, 137z, 138a, 138b, 138c, 138d, 138e, 138f, 138g, 138h, 138i, 138j, 138k, 138l, 138m, 138n, 138o, 138p, 138q, 138r, 138s, 138t, 138u, 138v, 138w, 138x, 138y, 138z, 139a, 139b, 139c, 139d, 139e, 139f, 139g, 139h, 139i, 139j, 139k, 139l, 139m, 139n, 139o, 139p, 139q, 139r, 139s, 139t, 139u, 139v, 139w, 139x, 139y, 139z, 140a, 140b, 140c, 140d, 140e, 140f, 140g, 140h, 140i, 140j, 140k, 140l, 140m, 140n, 140o, 140p, 140q, 140r, 140s, 140t, 140u, 140v, 140w, 140x, 140y, 140z, 141a, 141b, 141c, 141d, 141e, 141f, 141g, 141h, 141i, 141j, 141k, 141l, 141m, 141n, 141o, 141p, 141q, 141r, 141s, 141t, 141u, 141v, 141w, 141x, 141y, 141z, 142a, 142b, 142c, 142d, 142e, 142f, 142g, 142h, 142i, 142j, 142k, 142l, 142m, 142n, 142o, 142p, 142q, 142r, 142s, 142t, 142u, 142v, 142w, 142x, 142y, 142z, 143a, 143b, 143c, 143d, 143e, 143f, 143g, 143h, 143i, 143j, 143k, 143l, 143m, 143n, 143o, 143p, 143q, 143r, 143s, 143t, 143u, 143v, 143w, 143x, 143y, 143z, 144a, 144b, 144c, 144d, 144e, 144f, 144g, 144h, 144i, 144j, 144k, 144l, 144m, 144n, 144o, 144p, 144q, 144r, 144s, 144t, 144u, 144v, 144w, 144x, 144y, 144z, 145a, 145b, 145c, 145d, 145e, 145f, 145g, 145h, 145i, 145j, 145k, 145l, 145m, 145n, 145o, 145p, 145q, 145r, 145s, 145t, 145u, 145v, 145w, 145x, 145y, 145z, 146a, 146b, 146c, 146d, 146e, 146f, 146g, 146h, 146i, 146j, 146k, 146l, 146m, 146n, 146o, 146p, 146q, 146r, 146s, 146t, 146u, 146v, 146w, 146x, 146y, 146z, 147a, 147b, 147c, 147d, 147e, 147f, 147g, 147h, 147i, 147j, 147k, 147l, 147m, 147n, 147o, 147p, 147q, 147r, 147s, 147t, 147u, 147v, 147w, 147x, 147y, 147z, 148a, 148b, 148c, 148d, 148e, 148f, 148g, 148h, 148i, 148j, 148k, 148l, 148m, 148n, 148o, 148p, 148q, 148r, 148s, 148t, 148u, 148v, 148w, 148x, 148y, 148z, 149a,

1 b から SAM 1 0 5₁ ~ 1 0 5₄ にそれぞれセキュアコンテナ 1 0 4 a, 1 0 4 b を供給するようにしてもよい。

図 4 8 は、コンテンツプロバイダ 1 0 1 a, 1 0 1 b を用いる場合の第 1 実施形態の第 3 変形例に係わる EMD システムの構成図である。

この場合には、EMD サービスセンタ 1 0 2 は、コンテンツプロバイダ 1 0 1 a および 1 0 1 b に、それぞれ 6 カ月分の配信用鍵データ K D a₁ ~ K D a₆ および K D b₁ ~ K D b₆ を配信する。

また、EMD サービスセンタ 1 0 2 は、SAM 1 0 5₁ ~ 1 0 5₄ に、3 カ月分の配信用鍵データ K D a₁ ~ K D a₃ および K D b₁ ~ K D b₃ を配信する。

そして、コンテンツプロバイダ 1 0 1 a は、独自のコンテンツ鍵データ K c a を用いて暗号化したコンテンツファイル C F a と、コンテンツ鍵データ K c a および権利書データ 1 0 6 a などに対応する期間の配信用鍵データ K D a₁ ~ K D a₆ を用いて暗号化したキーファイル K F a とを格納したセキュアコンテナ 1 0 4 a を SAM 1 0 5₁ ~ 1 0 5₄ にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、EMD サービスセンタ 1 0 2 が配付するグローバルユニークな識別子 C o n t e n t _ I D が用いられ、EMD サービスセンタ 1 0 2 によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ 1 0 1 b は、独自のコンテンツ鍵データ K c b を用いて暗号化したコンテンツファイル C F b と、コンテンツ鍵データ K c b および権利書データ 1 0 6 b などに対応する期間の配信用鍵データ K D b₁ ~ K D b₆ を用いて暗号化したキーファイル K F b とを格納したセキュアコンテナ 1 0 4 b を SAM 1 0 5₁ ~ 1 0 5₄ にオンラインおよび／またはオフランで供給する。

SAM 1 0 5₁ ~ 1 0 5₄ は、セキュアコンテナ 1 0 4 a については、対応する期間の配信用鍵データ K D a₁ ~ K D a₆ を用いて復号を行い、所定の署名検

証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。

また、SAM105₁～105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKD_{b1}～KD_{b3}を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コンテンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKF_a, KF_bに対して、グローバルユニークな識別子Content_IDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 101bの公開鍵証明書データCER_{cpa}, CER_{cpb}を発行し、これに自らの署名データSIG_{1b, BSC}, SIG_{1a, BSC}を付してその正当性を認証する。

第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配

給する場合について説明する。

図48は、本実施形態のEMDシステム300の構成図である。

図48に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。

コンテンツプロバイダ301、EMDサービスセンタ302、SAM305₁～305₄およびサービスプロバイダ310は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。

また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505₁～505₄に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。

また、ユーザホームネットワーク303は、ネットワーク機器360₁およびAV機器360₂～360₄を有している。ネットワーク機器360₁はSAM305₁およびCAモジュール311を内蔵しており、AV機器360₂～360₄はそれぞれSAM305₂～305₄を内蔵している。

ここで、SAM305₁～305₄は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）308の作成を行なう点とを除いて、前述した第1実施形態のSAM105₁～105₄と同じである。

先ず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しよ

うとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106は、EMDサービスセンタ302に登録されて権威化(認証)される。

また、コンテンツプロバイダ301は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD_nを用いて、コンテンツ鍵データKcおよび権利書データ106を暗号化し、それらを格納したキーファイルKFを作成する。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納したセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ310に供給する。

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104が正当なコンテンツプロバイダ301によって作成されたものであるか、並びに送り主の正当性を確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格(SRP)に、自らのサービスの価格を加算した価格を示すプライスタグデータ(PT)312を作成する。

そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データK_{sp.s}による署名データとを格納したセキュアコンテナ304を作成する。

このとき、キーファイルKFは、配信用鍵データKD₁～KD₈によって暗号化されており、サービスプロバイダ310は当該配信用鍵データKD₁～KD₈を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。

また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

サービスプロバイダ310は、オンラインおよび／またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。

このとき、オフラインの場合には、セキュアコンテナ304はSAM305₁～305₄にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データK_{SBs}を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データK_{SBs}を用いて復号した後に、SAM305₁～305₄に転送する。

次に、SAM305₁～305₄において、セキュアコンテナ304を、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD₈を用いて復号した後に、署名データの検証処理を行う。

SAM305₁～305₄に供給されたセキュアコンテナ304は、ネットワーク機器360₁およびAV機器360₂～360₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM305₁～305₄は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。

利用履歴データ(履歴データまたは管理装置用履歴データ)308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク

303からEMDサービスセンタ302に送信される。

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決（計）算し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

本実施形態では、第1実施形態と同様に、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路（配送チャンネル）を介して提供されても、コンテンツデータC（商品）を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

また、本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密

鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ 301 の権利書データ 106 およびサービスプロバイダ 310 のプライスタグデータ 312 を登録して権威化することも、EMD サービスセンタ 302 の認証機能によるものである。

また、EMD サービスセンタ 302 は、例えば、配信用鍵データ $KD_1 \sim KD_n$ などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 が登録した権利書データ 106 と $SAM305_1 \sim SAM305_n$ から入力した利用履歴データ 308 とサービスプロバイダ 310 が登録したプライスタグデータ 312 とに基づいて、ユーザホームネットワーク 303 のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ 301 およびサービスプロバイダ 310 に分配して支払う権利処理（利益分配）機能を有する。

以下、コンテンツプロバイダ 301 の各構成要素について詳細に説明する。

〔コンテンツプロバイダ 301〕

図 50 は、コンテンツプロバイダ 301 の機能ブロック図であり、サービスプロバイダ 310 との間で送受信されるデータに関連するデータの流れが示されている。

図 50 に示すように、コンテンツプロバイダ 301 は、コンテンツマスタソースサーバ 111、電子透かし情報付加部 112、圧縮部 113、暗号化部 114、乱数発生部 115、暗号化部 116、署名処理部 117、セキュアコンテナ作成部 118、セキュアコンテナデータベース 118a、記憶部 119、相互認証部 120、暗号化・復号部 121、権利書データ作成部 122、EMD サービスセンタ管理部 125 およびサービスプロバイダ管理部 324 を有する。

図 50 において、図 2 と同一符号を付した構成要素は、前述した第 1 実施形態において図 2 および図 3 を参照しながら説明した同一符号の構成要素と同じであ

る。

すなわち、コンテンツプロバイダ301は、図2に示すSAM管理部124の代わりにサービスプロバイダ管理部324を設けた構成をしている。

サービスプロバイダ管理部324は、セキュアコンテナ作成部118から入力したセキュアコンテナ104を、オフラインおよび／またはオンラインで、図48に示すサービスプロバイダ310に提供する。セキュアコンテナ104には、第1実施形態と同様に、図4A、図4B、図4Cに示すコンテンツファイルCFおよびその署名データSIG_{8, CP}と、キーファイルKFおよびその署名データSIG_{7, CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1, BSC}とが格納されている。

サービスプロバイダ管理部324は、セキュアコンテナ104をオンラインでサービスプロバイダ310に配信する場合には、暗号化・復号部121においてセッション鍵データK_{SES}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してサービスプロバイダ310に配信する。

また、図3に示したコンテンツプロバイダ101内でのデータの流れは、サービスプロバイダ310にも同様に適用される。

〔サービスプロバイダ310〕

サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を、オンラインおよび／またはオフラインで、ユーザホームネットワーク303のネットワーク機器360₁およびAV機器360₂～360₄に配給する。

サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコン

コンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

図51は、サービスプロバイダ310の機能ブロック図である。

なお、図51には、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104に応じたセキュアコンテナ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。

図51に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部920を有する。

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図51および図52を参照しながら説明する。

図52は、当該処理のフローチャートである。

ステップSZ1：コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図4に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図50に示す相互認証部120と図51に示す相互認証部352との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

ステップSZ2：署名処理部354において、記憶部351に記憶されている

セキュアコンテナ104の図4Cに示す署名データ $SIG_{1, BSC}$ を、記憶部351から読み出したEMDサービスセンタ302の公開鍵データ $K_{BSC, P}$ を用いて検証し、その正当性が認められた後に、図4Cに示す公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP, P}$ を取り出す。

ステップSZ3：署名処理部354は、当該取り出した公開鍵データ $K_{CP, P}$ を用いて、記憶部351に記憶されているセキュアコンテナ104の図4A、図4Bに示す署名データ $SIG_{6, CP}$ 、 $SIG_{7, CP}$ の検証を行う。

ステップSZ4：プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、これをセキュアコンテナ作成部355に出力する。

ステップSZ5：署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{SP, P}$ を用いて、署名データ $SIG_{82, SP}$ 、 $SIG_{83, SP}$ 、 $SIG_{84, SP}$ を作成し、これをセキュアコンテナ作成部355に出力する。

ステップSZ6：セキュアコンテナ作成部355は、図53A～図53Dに示すように、コンテンツファイルCFおよびその署名データ $SIG_{82, SP}$ と、キーファイルKFおよびその署名データ $SIG_{83, BSC}$ と、プライスタグデータ312およびその署名データ $SIG_{84, SP}$ と、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{81, BSC}$ とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。そして、セキュアコンテナ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。

このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、そ

れらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MH E G (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合にはXML / SMIL / HTML (Hyper TextMarkup Language) プロトコルが用いられる。

このとき、コンテンツファイルCFおよびキーファイルKFは、コンテンツプロバイダ301によって一元的に管理され、セキュアコンテナ304を送信するプロトコルに依存しない。すなわち、コンテンツファイルCFおよびキーファイルKFは、MH E G および HTML のプロトコルをトンネリングした形でセキュアコンテナ304内に格納される。

ステップSZ7: ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび／またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データK_{SES}を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360₁に配信する。

なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}を

ワーク鍵データ K_w を暗号化し、ワーク鍵データ K_w をマスタ鍵データ K_M を用いて暗号化する。

そして、ユーザホームネットワーク管理部 357 は、セキュアコンテナ 304 と共に、スクランブル鍵データ K_{scr} およびワーク鍵データ K_w を、衛星を介してユーザホームネットワーク 303 に送信する。

また、例えば、マスタ鍵データ K_M を、ICカードなどに記憶してオフラインでユーザホームネットワーク 303 に配給する。

また、ユーザホームネットワーク管理部 357 は、ユーザホームネットワーク 303 から、当該サービスプロバイダ 310 が配給したコンテンツデータ C に関する SP 用購入履歴データ 309 を受信すると、これを記憶部 351 に書き込む。

サービスプロバイダ 310 は、将来のサービス内容を決定する際に、SP 用購入履歴データ 309 を参照する。また、ユーザ嗜好フィルタ生成部 920 は、SP 用購入履歴データ 309 に基づいて、当該 SP 用購入履歴データ 309 を送信した SAM 305₁ ~ 305₄ のユーザの嗜好を分析してユーザ嗜好フィルタデータ 900 を生成し、これをユーザホームネットワーク管理部 357 を介してユーザホームネットワーク 303 の CA モジュール 311 に送信する。

図 54 には、サービスプロバイダ 310 内における EMD サービスセンタ 302 との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ 310 の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMD サービスセンタ 302 に登録処理を行い、グローバルユニークな識別子 SP_ID を得ている。識別子 SP_ID は、記憶部 351 に記憶される。

まず、サービスプロバイダ 310 が、EMD サービスセンタ 302 に、自らの秘密鍵データ $K_{SP, s}$ に対応する公開鍵データ $K_{SP, s}$ の正当性を証明する公開鍵証

明書データ CER_{SP} を要求する場合の処理を図 5 4 を参照しながら説明する。

先ず、サービスプロバイダ 3 1 0 は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{SP, S}$ を生成し、当該秘密鍵データ $K_{SP, S}$ に対応する公開鍵データ $K_{SP, P}$ を作成して記憶部 3 5 1 に記憶する。

EMD サービスセンタ管理部 3 5 8、サービスプロバイダ 3 1 0 の識別子 SP_ID および公開鍵データ $K_{SP, P}$ を記憶部 3 5 1 から読み出す。

そして、EMD サービスセンタ管理部 3 5 8 は、識別子 SP_ID および公開鍵データ $K_{SP, P}$ を、EMD サービスセンタ 3 0 2 に送信する。

そして、EMD サービスセンタ管理部 3 4 8 は、当該登録に応じて、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{81, BSC}$ を EMD サービスセンタ 3 0 2 から入力して記憶部 3 5 1 に書き込む。

次に、サービスプロバイダ 3 1 0 が、EMD サービスセンタ 3 0 2 にプライスタグデータ 3 1 2 を登録して権威化する場合の処理を図 5 4 を参照して説明する。

この場合には、署名処理部 3 5 4 において、プライスタグデータ作成部 3 5 6 が作成したプライスタグデータ 3 1 2 と記憶部 3 5 1 から読み出したグローバルユニークな識別子 $Content_ID$ とを格納したモジュール Mod_{103} のハッシュ値が求められ、秘密鍵データ $K_{SP, S}$ を用いて署名データ $SIG_{80, SP}$ が生成される。

また、記憶部 3 5 1 から公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{81, BSC}$ が読み出される。

そして、図 5 5 に示すプライスタグ登録要求用モジュール Mod_{102} を、相互認証部 3 5 2 と EMD サービスセンタ 3 0 2 との間の相互認証によって得られたセッション鍵データ K_{SBS} を用いて暗号化・復号部 3 5 3 において暗号化した後に、EMD サービスセンタ管理部 3 5 8 から EMD サービスセンタ 3 0 2 に送信する。

なお、モジュールModiosに、サービスプロバイダ310のグローバルユニークな識別子SP_IDを格納してもよい。

また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信した決済レポートデータ307sを記憶部351に書き込む。

また、EMDサービスセンタ管理部358は、EMDサービスセンタ302から受信したマーケティング情報データ904を記憶部351に記憶する。

マーケティング情報データ904は、サービスプロバイダ310が今後配給するコンテンツデータCを決定する際に参考にされる。

〔EMDサービスセンタ302〕

EMDサービスセンタ302は、前述したように、認証局(CA:Certificate Authority)、鍵管理(Key Management)局および権利処理(Rights Clearing)局としての役割を果たす。

図56は、EMDサービスセンタ302の機能の構成図である。

図56に示すように、EMDサービスセンタ302は、鍵サーバ141、鍵データベース141a、決済処理部442、署名処理部443、決算機関管理部144、証明書・権利書管理部445、CERデータベース445a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151、サービスプロバイダ管理部390、SPデータベース390a、ユーザ嗜好フィルタ生成部901およびマーケティング情報データ生成部902を有する。

図56において、図10および図11と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

以下、図56において、新たな符号を付した機能ブロックについて説明する。

なお、図56には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

また、図57には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ301との間で送受信されるデータに関連するデータの流れが示されている。

また、図58には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、図49に示すSAM305₁～305₄および決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

決済処理部442は、図58に示すように、SAM305₁～305₄から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312に基づいて決済処理を行う。なお、この際に、決済処理部442は、サービスプロバイダ310によるダンプの有無などを監視する。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図56および図58に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

ここで、決済請求権データ152c、152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図59に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ304に格納されたコンテンツデータCを提供

したコンテンツプロバイダ 301 の識別子 CP_ID、セキュアコンテナ 304 を配給したサービスプロバイダ 310 の識別子 SP_ID、コンテンツデータ C の信号諸元データ、セキュアコンテナ 304 内のコンテンツデータ C の圧縮方法、セキュアコンテナ 304 を記録した記録媒体の識別子 Media_ID、セキュアコンテナ 304 を配給を受けた SAM 305₁ ~ 305₄ の識別子 SAM_ID、当該 SAM 105₁ ~ 105₄ のユーザの USER_ID などが記述されている。従って、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク 303 のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

証明書・権利書管理部 445 は、CER データベース 445 a に登録されて権威化された公開鍵証明書データ CER_{cp}、公開鍵証明書データ CER_{sp} および公開鍵証明書データ CER_{sam1} ~ CER_{sam2} などを読み出すと共に、コンテンツプロバイダ 301 の権利書データ 106 およびコンテンツ鍵データ K_c、並びにサービスプロバイダ 310 のプライスタグデータ 312 など CER データベース 445 a に登録して権威化する。

このとき、証明書・権利書管理部 445 は、権利書データ 106、コンテンツ鍵データ K_c およびプライスタグデータ 312 などのハッシュ値をとり、秘密鍵データ K_{esc, s} を用いた署名データを付して権威化証明書データを作成する。

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されているコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148 a にアクセスできる。

ユーザ嗜好フィルタ生成部 901 は、利用履歴データ 308 に基づいて、当該利用履歴データ 308 を送信した SAM 305₁ ~ 305₄ のユーザの嗜好に応

じたコンテンツデータCを選択するためのユーザ嗜好フィルタデータ903を生成し、ユーザ嗜好フィルタデータ903をSAM管理部149を介して、当該利用履歴データ308を送信したSAM305₁～305₄に送信する。

マーケティング情報データ生成部902は、利用履歴データ308に基づいて、例えば、複数のサービスプロバイダ310によってユーザホームネットワーク103に配給されたコンテンツデータCの全体の購入状況などを示すマーケティング情報データ904を生成し、これをサービスプロバイダ管理部390を介して、サービスプロバイダ310に送信する。サービスプロバイダ310は、マーケティング情報データ904を参考にして、今後提供するサービスの内容を決定する。

以下、EMDサービスセンタ302内での処理の流れを説明する。

EMDサービスセンタ302からコンテンツプロバイダ301への配信用鍵データKD₁～KD₉の送信と、EMDサービスセンタ302からSAM305₁～305₄への配信用鍵データKD₁～KD₉の送信とは、第1実施形態の場合と同様に行なわれる。

また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部445がCERデータベース445aに対して登録を行なう点を除いて、前述した第1実施形態の場合と同様に行なわれる。

以下、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図56および図60を参照しながら説明する。

図60は、当該処理のフローチャートである。

ステップS01：サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子SP_ID、公開鍵データK_{SP, P}および署名データSIG_{70, SP}を含む公開鍵証明書データ登

録要求をサービスプロバイダ310から受信すると、これらを、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

ステップS02：当該復号した署名データ $SIG_{70, SP}$ の正当性を署名処理部443において確認した後に、識別子 SP_ID および公開鍵データ $K_{SP, P}$ に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。

ステップS03：証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データ CER_{SP} をCERデータベース445aから読み出してサービスプロバイダ管理部390に出力する。

ステップS04：署名処理部443は、公開鍵証明書データ CER_{SP} のハッシュ値をとり、EMDサービスセンタ302の秘密鍵データ $K_{ESC, S}$ を用いて、署名データ $SIG_{81, ESC}$ を作成し、これをサービスプロバイダ管理部390に出力する。

ステップS05：サービスプロバイダ管理部390は、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{81, ESC}$ を、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ310に送信する。

なお、EMDサービスセンタ302がSAM105₁～105₄から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106の登録要求を受けた場合の処理も、第1実施形態と同様である。

次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図56および図61を参照しながら説明する。

図61は、当該処理のフローチャートである。

ステップSP1：サービスプロバイダ管理部380がサービスプロバイダ310から図55に示すプライスタグ登録要求モジュールMod₁₀₂を受信すると、相互認証部150と図51に示す相互認証部352との間の相互認証で得られたセッション鍵データK_{SBS}を用いてプライスタグ登録要求モジュールMod₁₀₂を復号する。

ステップSP2：当該復号したプライスタグ登録要求モジュールMod₁₀₂に格納された署名データSIG_{80, SP}の正当性を署名処理部443において確認する。

ステップSP3：証明書・権利書管理部445は、プライスタグ登録要求モジュールMod₁₀₂に格納されたプライスタグデータ312を、CERデータベース445aに登録して権威化する。

次に、EMDサービスセンタ302において決済を行なう場合の処理を図58および図62を参照しながら説明する。

図62は、当該処理のフローチャートである。

ステップSQ1：SAM管理部149は、ユーザホームネットワーク303の例えばSAM305₁から利用履歴データ308およびその署名データSIG_{205, SAM1}を入力すると、利用履歴データ308および署名データSIG_{205, SAM1}を、相互認証部150とSAM305₁～305₄との間の相互認証によって得られたセッション鍵データK_{SBS}を用いて復号し、SAM305₁の公開鍵データK_{SAM1, P}を用いて署名データSIG_{205, SAM1}の検証を行なった後に、決算処理部442に出力する。

ステップSQ2：決済処理部442は、SAM305₁から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ1

52cと、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sとを作成する。

なお、決済処理部442による決済処理は、利用履歴データ308を入力する毎に行ってもよいし、所定の期間毎に行ってもよい。

ステップSQ3：図56および図58に示すように、コンテンツプロバイダ301およびサービスプロバイダ310についての決済請求権データ152c, 152sを作成し、これらを決算機関管理部144に出力する。

決算機関管理部144は、決済請求権データ152c, 152sと、それらについて秘密鍵データ $K_{ESC, s}$ を用いて作成した署名データとを、相互認証およびセッション鍵データ K_{SES} による復号を行なった後に、図49に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

なお、EMDサービスセンタ302は、決済請求権データ152c, 152sをそれぞれコンテンツプロバイダ301およびサービスプロバイダ310に送信してもよい。この場合には、コンテンツプロバイダ301およびサービスプロバイダ310が、当該受信した決済請求権データ152c, 152sに基づいて決済機関91に金銭を請求する。

ステップSQ4：コンテンツプロバイダ301およびサービスプロバイダ310についての決済レポートデータS307c, S307sが、それぞれコンテンツプロバイダ管理部148およびサービスプロバイダ管理部390を介して、コンテンツプロバイダ301およびサービスプロバイダ310に出力される。

EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM305₁～305₄の出荷時の処理と、SAM登録リストの登録処理とを行なう。

〔ユーザホームネットワーク 303〕

ユーザホームネットワーク 303 は、図 49 に示すように、ネットワーク機器 360₁ および A/V 機器 360₂ ~ 360₄ を有している。

ネットワーク機器 360₁ は、CA モジュール 311 および SAM 305₁ を内蔵している。また、A/V 機器 360₂ ~ 360₄ は、それぞれ SAM 305₂ ~ 305₄ を内蔵している。

SAM 305₁ ~ 305₄ の相互間は、例えば、1394 シリアルインタフェースバスなどのバス 191 を介して接続されている。

なお、A/V 機器 360₂ ~ 360₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス 191 を介してネットワーク機器 360₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク 303 は、ネットワーク機能を有していない A/V 機器のみを有していてもよい。

以下、ネットワーク機器 360₁ について説明する。

図 63 は、ネットワーク機器 360₁ の構成図である。

図 63 に示すように、ネットワーク機器 360₁ は、通信モジュール 162、CA モジュール 311、復号モジュール 905、SAM 305₁、復号・伸長モジュール 163、購入・利用形態決定操作部 165、ダウンロードメモリ 167、再生モジュール 169 および外部メモリ 201 を有する。

図 63 において、図 16 と同一符号を付した構成要素は、第 1 実施形態で説明した同一符号の構成要素と同じである。

通信モジュール 162 は、サービスプロバイダ 310 との間の通信処理を行なう。

具体的には、通信モジュール 162 は、サービスプロバイダ 310 から衛星放送などで受信したセキュアコンテナ 304 を復号モジュール 905 に出力する。また、通信モジュール 162 は、サービスプロバイダ 310 に電話回線などを介

してSP用購入履歴データ309を受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

図64は、CAモジュール311および復号モジュール905の機能ブロック図である。

図64に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。

相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との間で相互認証を行ってセッション鍵データ K_{SBS} を生成し、これを暗号化・復号部908に出力する。

記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力し、記憶部907から読み出したマスタ鍵データ K_M を用いてワーク鍵データ K_W を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データ K_W を用いてスクランブル鍵データ K_{SCR} を復号し、当該復号したスクランブル鍵データ K_{SCR} を復号部910に出力する。

また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データ K_{SBS} を用いて復号して復号モジュール905のセキュアコンテナ選択部911に出力する。

また、暗号化・復号部 908 は、SP 用購入履歴データ生成部 909 から入力した SP 用購入履歴データ 309 を、相互認証部 906 からのセッション鍵データ K_{SSS} を用いて復号して通信モジュール 162 を介してサービスプロバイダ 310 に送信する。

SP 用購入履歴データ生成部 909 は、図 63 に示す購入・利用形態決定操作部 165 を用いてユーザによるコンテンツデータ C の購入操作に応じた操作信号 S165、または SAM305₁ からの利用制御状態データ 166 に基づいて、サービスプロバイダ 310 に固有のコンテンツデータ C の購入履歴を示す SP 用購入履歴データ 309 を生成し、これを暗号化・復号部 908 に出力する。

SP 用購入履歴データ 309 は、例えば、サービスプロバイダ 310 が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

なお、CA モジュール 311 は、サービスプロバイダ 310 が課金機能を有している場合には、サービスプロバイダ 310 の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CA モジュール 311 は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ 310 に送信する。

復号モジュール 905 は、復号部 910 およびセキュアコンテナ選択部 911 を有する。

復号部 910 は、通信モジュール 162 から、それぞれ暗号化されたセキュアコンテナ 304、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力する。

そして、復号部 910 は、暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を CA モジュール 311 の暗号化・復号部 908 に出力し、暗号化・復号部 908 から復号されたスクランブル鍵データ K_{SCR} を入力する。

そして、復号部 910 は、暗号化されたセキュアコンテナ 304 を、スクラン

ブル鍵データ K_{scr} を用いて復号した後に、セキュアコンテナ選択部 911 に出力する。

なお、セキュアコンテナ 304 が、MPEG2 Transport Stream 方式でサービスプロバイダ 310 から送信される場合には、例えば、復号部 910 は、TS Packet 内の ECM (Entitlement Control Message) からスクランブル鍵データ K_{scr} を取り出し、EMM (Entitlement Management Message) からワーク鍵データ K_w を取り出す。

ECM には、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMM は、その他に、ユーザ（視聴者）毎に異なる個別試験契約情報などが含まれている。

セキュアコンテナ選択部 911 は、復号部 910 から入力したセキュアコンテナ 304 を、CA モジュール 311 から入力したユーザ嗜好フィルタデータ 900 を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ 304 を選択して SAM 305₁ に出力する。

次に、SAM 305₁ について説明する。

なお、SAM 305₁ は、サービスプロバイダ 310 についての署名検証処理を行なうなど、コンテンツプロバイダ 301 に加えてサービスプロバイダ 310 に関する処理を行う点を除いて、図 17～図 41 を用いて前述した第 1 実施形態の SAM 105₁ と基本的に行なう機能および構造を有している。

また、SAM 305₂～305₄ は、SAM 305₁ と基本的に同じ機能を有している。

すなわち、SAM 305₁～305₄ は、コンテンツ単位の課金処理をおこなうモジュールであり、EMD サービスセンタ 302 との間で通信を行う。

以下、SAM 305₁ の機能について詳細に説明する。

図 65 は、SAM 305₁ の機能の構成図である。

なお、図 65 には、サービスプロバイダ 310 からセキュアコンテナ 304 を

入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図65に示すように、SAM305₁は、相互認証部170、暗号化・復号部171、172、173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。

なお、図65に示すSAM305₁の所定の機能は、SAM105₁の場合と同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図65において、図17と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

また、図63に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。

また、スタックメモリ200には、図66に示すように、コンテンツ鍵データK_c、権利書データ(UCP)106、記憶部192のロック鍵データK_{loc}、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}、サービスプロバイダ310の公開鍵証明書データCER_{SP}、利用制御状態データ(UCS)366、SAMプログラム・ダウンロード・コンテナSDC₁～SDC₉およびプライスタグデータ312などが記憶される。

以下、SAM305₁の機能ブロックのうち、図65において新たに符号を付した機能ブロックについて説明する。

署名処理部589は、記憶部192あるいはスタックメモリ200から読み出したEMDサービスセンタ302の公開鍵データK_{BSC.P}、コンテンツプロバイ

ダ 3 0 1 の公開鍵データ $K_{cp, p}$ およびサービスプロバイダ 3 1 0 の公開鍵データ $K_{sp, p}$ を用いて、セキュアコンテナ 3 0 4 内の署名データの検証を行なう。

課金処理部 5 8 7 は、図 6 7 に示すように、図 6 3 に示す購入・利用形態決定操作部 1 6 5 からの操作信号 $S 1 6 5$ と、スタックメモリ 2 0 0 から読み出されたプライスタグデータ 3 1 2 とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部 5 8 7 による課金処理は、利用監視部 1 8 6 の監視の下、権利書データ 1 0 6 が示す使用許諾条件などの権利内容および利用制御状態データ 1 6 6 に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

また、課金処理部 5 8 7 は、課金処理において、利用履歴データ 3 0 8 を生成し、これを外部メモリ管理部 8 1 1 を介して外部メモリ 2 0 1 に書き込む。

ここで、利用履歴データ 3 0 8 は、第 1 実施形態の利用履歴データ 1 0 8 と同様に、EMD サービスセンタ 3 0 2 において、セキュアコンテナ 3 0 4 に関連したライセンス料の支払いを決定する際に用いられる。

また、課金処理部 5 8 7 は、操作信号 $S 1 6 5$ に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ 1 6 6 を生成し、これを外部メモリ管理部 8 1 1 を介して外部メモリ 2 0 1 に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ 1 6 6 は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ 1 6 6 には、コンテンツの ID、購入形態、買い切り価格、当該コン

テンツの購入が行なわれたSAMのSAM_ID, 購入を行なったユーザのUSER_IDなどが記述されている。

なお、決定された購入形態が再生課金である場合には、例えば、SAM305₁からサービスプロバイダ310に利用制御状態データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ108をSAM105₁に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

また、SAM305₁では、EMDサービスセンタ管理部185がEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図63に示す復号モジュール905から入力したセキュアコンテナ304が、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM305₁において、当該SAM305₁のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

以下、SAM305₁内での処理の流れを説明する。

EMDサービスセンタ302から受信した配信用鍵データKD₁～KD₉を記憶部192に格納する際のSAM305₁内での処理の流れは、前述したSAM105₁の場合と同様である。

以下、セキュアコンテナ304をサービスプロバイダ310から入力し、セキュアコンテナ304内のキーファイルKFを復号する際のSAM305₁内での

処理の流れを図65および図68を参照しながら説明する。

図68は、当該処理のフローチャートである。

ステップSR1：相互認証部170と図51に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図53A～図53Dに示すセキュアコンテナ304を復号する。

ステップSR2：署名処理部589は、図53Dに示す署名データ $SIG_{81, E}$ 、 sc の検証を行なった後に、図53Dに示す公開鍵証明書データ CER_{SP} 内に格納されたサービスプロバイダ310の公開鍵データ $K_{SP, P}$ を用いて、署名データ $SIG_{82, SP}$ 、 $SIG_{83, SP}$ 、 $SIG_{84, SP}$ の正当性を確認する。

サービスプロバイダ管理部580は、署名データ $SIG_{82, SP}$ 、 $SIG_{83, SP}$ 、 $SIG_{84, SP}$ の正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

ステップSR3：ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

ステップSR4：ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図53Bに示すキーファイルKFを読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_9$ を用いて、キーファイルKFを復号する。

。

ステップSR5：セキュアコンテナ復号部183は、図53Bに示す署名・証明書モジュールMod1に格納された署名データSIG_{1, BSC}、SIG_{2, CP}～SIG_{4, CP}を署名処理部589に出力する。

署名処理部589は、図53Bに示す署名データSIG_{1, BSC}の検証を行なった後に、公開鍵証明書データCER_{CP}内に格納された公開鍵データK_{CP, P}を用いて署名データSIG_{2, CP}～SIG_{4, CP}の検証を行なう。

ステップSR6：セキュアコンテナ復号部183は、署名データSIG_{2, CP}～SIG_{4, CP}の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図67および図69を参照しながら説明する。

図69は、当該処理のフローチャートである。

ステップSS1：課金処理部587において、ユーザによる図63に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が入力されたか否かが判断され、入力されたと判断された場合にはステップSS2の処理が実行され、そうでない場合にはステップSS3の処理が実行される。

。

ステップSS2：例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図63に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SBs}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{SBs}による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図63に示す復号部221において復号された後に、復号部222に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcおよび半開示パラメータデータ199が、図63に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データKcおよび半開示パラメータデータ199に対してセッション鍵データKsesによる暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データKcを用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール168において再生され、コンテンツデータCに応じた音響が出力される。

ステップSS3：コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

ステップSS4：課金処理部187において、決定された購入形態に応じた利用履歴データ308および利用制御状態データ166が生成され、利用履歴データ308が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

ステップSS5：スタックメモリ200に格納されているキーファイルKFに

、利用制御状態データ 166 が加えられ、購入形態が決定した後述する図 7 1 に示す新たなキーファイル KF_{11} が生成される。キーファイル KF_{11} は、スタックメモリ 200 に記憶される。

図 7 1 に示すように、キーファイル KF_1 に格納された利用制御状態データ 166 はストレージ鍵データ K_{STR} を用いて DES の CBC モードを利用して暗号化されている。また、当該ストレージ鍵データ K_{STR} を MAC 鍵データとして用いて生成した MAC 値である MAC_{900} が付されている。また、利用制御状態データ 166 および MAC_{900} からなるモジュールは、メディア鍵データ K_{MED} を用いて DES の CBC モードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ K_{MED} を MAC 鍵データとして用いて生成した MAC 値である MAC_{901} が付されている。

次に、ダウンロードメモリ 167 に記憶されている購入形態が既に決定されたコンテンツデータ C を再生する場合の処理の流れを、図 6 7 および図 7 0 を参照しながら説明する。

図 7 0 は、当該処理のフローチャートである。

ステップ ST 1 : 例えば、ユーザによる操作に応じて、再生対象となるコンテンツの指定を SAM が受ける。

ステップ ST 2 : 利用監視部 186 の監視下で、操作信号 S165 に基づいて、ダウンロードメモリ 167 に記憶されているコンテンツファイル CF が読み出される。

ステップ ST 3 : 当該読み出されたコンテンツファイル CF が、図 6 3 に示す復号・伸長モジュール 163 に出力される。

また、スタックメモリ 200 から読み出されたコンテンツ鍵データ K_c が復号・伸長モジュール 163 に出力される。

ステップ ST 4 : 復号・伸長モジュール 163 の復号部 222 において、コンテンツ鍵データ K_c を用いたコンテンツファイル CF の復号と、伸長部 223 に

よる伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

ステップST5：課金処理部587において、操作信号S165に応じて、利用履歴データ308が更新される。

利用履歴データ308は、秘密鍵データ $K_{SAM1, s}$ を用いて作成したそれぞれ署名データ $SIG_{205, SAM1}$ と共に、EMDサービスセンタ管理部185を介して、所定のタイミングで、EMDサービスセンタ302に送信される。

以下、図72に示すように、例えば、ネットワーク機器360₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFを、バス191を介して、AV機器360₂のSAM305₂に転送する場合のSAM305₁内での処理の流れを図73および図74を参照しながら説明する。

ステップSU1：ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器360₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

これにより、課金処理部587は、操作信号S165に基づいて、スタックメモリ200に記憶されている利用履歴データ308を更新する。

ステップSU2：ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図75Aに示すコンテンツファイルCFをSAM管理部190に出力する。

ステップSU3：スタックメモリ200から読み出した図75Bに示す既に購入形態が決定されたキーファイル KF_{11} を、署名処理部588およびSAM管理部190に出力する。

ステップSU4：署名処理部588は、キーファイル KF_{11} の署名データ $SIG_{80, SAM1}$ を作成し、これをSAM管理部190に出力する。

ステップSU5：SAM管理部190は、記憶部192から、図75Cに示す公開鍵証明書データ CER_{SAM1} およびその署名データ $SIG_{22, BSC}$ を読み出す。

また、相互認証部170は、SAM305₂との間で相互認証を行って得たセッション鍵データ K_{SES} を暗号化・復号部171に出力する。

SAM管理部190は、図75A, B, Cに示すデータからなるセキュアコンテナを作成する。

ステップSU6：暗号化・復号部171において、セッション鍵データ K_{SES} を用いて当該セキュアコンテナを暗号化して作成して、図73に示すAV機器360₂のSAM305₂に出力する。

以下、図72に示すように、SAM305₁から入力したコンテンツファイルCFなどを、RAM型などの記録媒体（メディア）に書き込む際のSAM305₂内での処理の流れを、図76および図77を参照しながら説明する。

図77は、当該処理のフローチャートである。

ステップSV1：SAM305₂のSAM管理部190は、図76に示すように、図75Aに示すコンテンツファイルCF、図75Bに示すキーファイル KF_{11} およびその署名データ $SIG_{80, SAM1}$ と、図75Cに示す公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22, BSC}$ とを、ネットワーク機器360₁のSAM305₁から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイル KF_{11} およびその署名データ $SIG_{80, SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22, BSC}$ とが、相互認証部170とSAM305₁の相互認証部170との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて復号される。

次に、セッション鍵データ K_{SES} を用いて復号されたコンテンツファイルCFがメディアSAM管理部197に出力される。

また、セッション鍵データ K_{SES} を用いて復号されたキーファイル KF_{11} およ

びその署名データ $SIG_{80, SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22, BSC}$ とが、スタックメモリ 200 に書き込まれる。

ステップSV2：署名処理部 589 は、スタックメモリ 200 から読み出した署名データ $SIG_{22, BSC}$ を、記憶部 192 から読み出した公開鍵データ $K_{BSC, P}$ を用いて検証して、公開鍵証明書データ CER_{SAM1} の正当性を確認する。

そして、署名処理部 589 は、公開鍵証明書データ CER_{SAM1} の正当性を確認すると、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1, P}$ を用いて、署名データ $SIG_{80, SAM1}$ の正当性を確認する。

ステップSV3：署名データ $SIG_{80, SAM1}$ の正当性を確認されると、図 75 B に示すキーファイル KF_{11} をスタックメモリ 200 から読み出して暗号化・復号部 173 に出力する。

そして、暗号化・復号部 173 は、記憶部 192 から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いてキーファイル KF_{11} を順に暗号化してメディア SAM 管理部 197 に出力する。

ステップSV4：メディア SAM 管理部 197 は、SAM 管理部 190 から入力したコンテンツファイル CF および暗号化・復号部 173 から入力したキーファイル KF_{11} を、図 72 に示す記録モジュール 260 に出力する。

そして、記録モジュール 260 は、メディア SAM 管理部 197 から入力したコンテンツファイル CF およびキーファイル KF_{11} を、図 72 に示す RAM 型の記録媒体 250 の RAM 領域 251 に書き込む。

なお、SAM 305₁ 内での処理のうち、コンテンツの購入形態が未決定の ROM 型の記録媒体の購入形態を決定する際の AV 機器 360₂ 内での処理の流れ、AV 機器 360₂ において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナ 304 を読み出してこれを AV 機器 360₂ に転送して RAM 型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ 310 の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキー

ファイル内にプライスタグデータ 312 を格納する点を除いて、第 1 実施形態の SAM105₁ の場合と同じである。

次に、図 4 8 に示す EMD システム 300 の全体動作について説明する。

図 7 8 および図 7 9 は、EMD システム 300 の全体動作のフローチャートである。

ここでは、サービスプロバイダ 310 からユーザホームネットワーク 303 にオンラインでセキュアコンテナ 304 を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMD サービスセンタ 302 へのコンテンツプロバイダ 301、サービスプロバイダ 310 および SAM305₁ ~ 305₄ の登録は既に終了しているものとする。

ステップ S21: EMD サービスセンタ 302 は、コンテンツプロバイダ 301 の公開鍵データ $K_{CP, P}$ の公開鍵証明書 CER_{CP} を、自らの署名データ $SIG_{1, BSC}$ と共にコンテンツプロバイダ 301 に送信する。

また、EMD サービスセンタ 302 は、コンテンツプロバイダ 301 の公開鍵データ $K_{SP, P}$ の公開鍵証明書 CER_{SP} を、自らの署名データ $SIG_{1, BSC}$ と共にサービスプロバイダ 310 に送信する。

また、EMD サービスセンタ 302 は、各々有効期限が 1 カ月の 6 カ月分の配信用鍵データ $KD_1 \sim KD_6$ をコンテンツプロバイダ 301 に送信し、3 カ月分の配信用鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク 303 の SAM305₁ ~ 305₄ に送信する。

ステップ S22: コンテンツプロバイダ 301 は、図 7 A に示す権利登録要求モジュール Mod_2 を、EMD サービスセンタ 302 に送信する。

そして、EMD サービスセンタ 302 は、所定の署名検証を行った後に、権利書データ 106 およびコンテンツ鍵データ K_c を登録して権威化（認証）する。

ステップ S23: コンテンツプロバイダ 301 は、署名データの作成処理や、SIG 対応する期間の配信用鍵データ $KD_1 \sim KD_6$ などを用いた暗号化処理を

経て、図 4 A、図 4 B、図 4 C に示すデータを格納したセキュアコンテナ 1 0 4 を、サービスプロバイダ 3 1 0 に供給する。

ステップ S 2 4 : サービスプロバイダ 3 1 0 は、図 4 C に示す署名データ $SIG_{1, BSC}$ を検証した後に、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP, P}$ を用いて、図 4 A、B に示す署名データ $SIG_{1, CP}$ および $SIG_{7, CP}$ を検証して、セキュアコンテナ 1 0 4 が正当なコンテンツプロバイダ 3 0 1 から送信されたものであるかを確認する。

ステップ S 2 5 : サービスプロバイダ 3 1 0 は、プライスタグデータ 3 1 2 を作成し、プライスタグデータ 3 1 2 を格納した図 5 3 に示すセキュアコンテナ 3 0 4 を作成する。

ステップ S 2 6 : サービスプロバイダ 3 1 0 は、図 5 5 に示すプライスタグ登録要求モジュール Mod_{102} を、EMD サービスセンタ 3 0 2 に送信する。

そして、EMD サービスセンタ 3 0 2 は、所定の署名検証を行った後に、プライスタグデータ 3 1 2 を登録して権威化する。

ステップ S 2 7 : サービスプロバイダ 3 1 0 は、例えば、ユーザホームネットワーク 3 0 3 の CA モジュール 3 1 1 からの要求に応じて、ステップ S 2 5 で作成したセキュアコンテナ 3 0 4 を、オンラインあるいはオフラインで、図 6 3 に示すネットワーク機器 3 6 0₁ の復号モジュール 3 0 5 に送信する。

ステップ S 2 8 : CA モジュール 3 1 1 は、SP 用購入履歴データ 3 0 9 を作成し、これを所定のタイミングで、サービスプロバイダ 3 1 0 に送信する。

ステップ S 2 9 : SAM 3 0 5₁ ~ 3 0 5₄ のいずれかにおいて、図 5 3 D に示す署名データ $SIG_{1, BSC}$ を検証した後に、公開鍵証明書データ CER_{SP} に格納された公開鍵データ $K_{SP, P}$ を用いて、図 5 3 A、B、C に示す署名データ $SIG_{1, SP}$ 、 $SIG_{2, SP}$ 、 $SIG_{3, SP}$ 、 $SIG_{4, SP}$ を検証して、セキュアコンテナ 3 0 4 が正当なサービスプロバイダ 3 1 0 から送信されたものであるかを確認する。

ステップ S 3 0 : SAM 3 0 5₁ ~ 3 0 5₄ のいずれかにおいて、配信用鍵デ

ータKD₁ ~ KD₃を用いて、図53Bに示すキーファイルKFを復号する。そして、SAM305₁ ~ 305₄のいずれかにおいて、図53Bに示す署名データSIG_{1, BSC}を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP, P}を用いて、図53Bに示す署名データSIG_{2, CP}, SIG_{3, CP}およびSIG_{4, CP}を検証して、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106が正当なコンテンツプロバイダ301によって作成されたものであるかを確認する。

ステップS31：ユーザが図63の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

ステップS32：ステップS31において生成された操作信号S165に基づいて、SAM305₁ ~ 305₄において、セキュアコンテナ304の利用履歴(Usage Log)データ308が生成される。

SAM305₁ ~ 305₄からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG_{205, SAM1}が送信される。

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152_c, 152_sを作成する。

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152_c, 152_sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の所有者に分配される。

以上説明したように、EMDシステム300では、図4に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキ

ーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305₁～305₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₅を用いて暗号化されており、配信鍵データKD₁～KD₅を保持しているSAM305₁～305₄内でのみ復号される。そして、SAM305₁～305₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300にれば、権利書データ106をサービスプロバイダ310が管理できないようできる。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303における当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305₁～305₄におけるコンテンツデータCの権利処理を共通化できる。

また、EMDシステム300では、ユーザホームネットワーク303内のネッ

トワーク機器 360₁、およびAV機器 360₂～360₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₄に供給される。従って、SAM305₁～305₄において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

第2実施形態の第1変形例

図80は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。

図80において、図49と同一符号を付した構成要素は、第2実施形態で説明した同一符号の構成要素と同じである。

図80に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

サービスプロバイダ 310 a は、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータ C と、当該コンテンツデータ C について独自に作成したプライスタグデータ 312 a とを格納したセキュアコンテナ 304 a を作成し、これをネットワーク機器 360₁ に配給する。

また、サービスプロバイダ 310 b は、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータ C と、当該コンテンツデータ C について独自に作成したプライスタグデータ 312 b とを格納したセキュアコンテナ 304 b を作成し、これをネットワーク機器 360₁ に配給する。

ここで、セキュアコンテナ 304 a, 304 b のフォーマットは、図 53 を用いた説明したセキュアコンテナ 304 と同じである。

ネットワーク機器 360 a₁ には、サービスプロバイダ 310 a, 310 b の各々に対応した CA モジュール 311 a, 311 b が設けられている。

CA モジュール 311 a, 311 b は、自らの要求に応じたセキュアコンテナ 304 a, 304 b の配給を、それぞれサービスプロバイダ 310 a, 310 b から受ける。

次に、CA モジュール 311 a, 311 b は、配給されたセキュアコンテナ 304 a, 304 b に応じた SP 用購入履歴データ 309 a, 309 b をそれぞれ作成し、これらをそれぞれサービスプロバイダ 310 a, 310 b に送信する。

また、CA モジュール 311 a, 311 b は、セキュアコンテナ 304 a, 304 b をセッション鍵データ K_{SES} で復号した後に、SAM 305₁ ~ 305₄ に出力する。

次に、SAM 305₁ ~ 305₄ において、共通の配信用鍵データ K_{D1} ~ K_{D3} を用いて、セキュアコンテナ 304 a, 304 b 内のキーファイル K_F が復号され、共通の権利書データ 106 に基づいて、ユーザからの操作に応じたコン

テンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ 308 が作成される。

そして、SAM 305₁ ~ 305₄ から EMD サービスセンタ 302 に、利用履歴データ 308 が送信される。

EMD サービスセンタ 302 では、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 およびサービスプロバイダ 310 a, 310 b の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152 c, 152 s a, 152 s b を作成する。

EMD サービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152 c, 152 s a, 152 s b を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301 およびサービスプロバイダ 310 a, 310 b の所有者に分配される。

上述したように、EMD システム 300 b によれば、同じコンテンツファイル CF をサービスプロバイダに 310 a, 310 b に供給する場合に、当該コンテンツファイル CF についての権利書データ 106 を配信用鍵データ KD₁ ~ KD₄ で暗号化してサービスプロバイダに 310 a, 310 b に供給し、サービスプロバイダに 310 a, 310 b は暗号化された権利書データ 106 をそのまま格納したセキュアコンテナ 304 a, 304 b をユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内の SAM 305₁ ~ 305₄ では、コンテンツファイル CF をサービスプロバイダに 310 a, 310 b の何れから配給を受けた場合でも、共通の権利書データ 106 に基づいて権利処理を行うことができる。

なお、上述した第 1 変形例では、2 個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

第 2 実施形態の第 2 変形例

図 8 1 は、第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いた EMD システム 3 0 0 b の構成図である。

図 8 1 において、図 4 9 と同一符号を付した構成要素は、第 2 実施形態で説明した同一符号の構成要素と同じである。

図 8 1 に示すように、EMD システム 3 0 0 b では、コンテンツプロバイダ 3 0 1 a, 3 0 1 b からサービスプロバイダ 3 1 0 に、それぞれセキュアコンテナ 1 0 4 a, 1 0 4 b が供給される。

サービスプロバイダ 3 1 0 は、例えば、コンテンツプロバイダ 3 0 1 a, 3 0 1 b が供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ 1 0 4 a についてのプライスタグデータ 3 1 2 a と、セキュアコンテナ 1 0 4 b についてのプライスタグデータ 3 1 2 b とをそれぞれ生成し、これらを格納したセキュアコンテナ 3 0 4 c を作成する。

図 8 1 に示すように、セキュアコンテナ 3 0 4 c には、コンテンツファイル C F a, C F b、キーファイル K F a, K F b、プライスタグデータ 3 1 2 a, 3 1 2 b、それらの各々についてのサービスプロバイダ 3 1 0 の秘密鍵データ K_{cp} s による署名データが格納されている。

セキュアコンテナ 3 0 4 c は、ユーザホームネットワーク 3 0 3 のネットワーク機器 3 6 0₁ の C A モジュール 3 1 1 で受信された後に、S A M 3 0 5₁ ~ 3 0 5₄ において処理される。

S A M 3 0 5₁ ~ 3 0 5₄ では、配信用鍵データ $K D a_1$ ~ $K D a_4$ を用いて、キーファイル K F a が復号され、権利書データ 1 0 6 a に基づいて、コンテンツファイル C F a についてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ 3 0 8 に記述される。

また、S A M 3 0 5₁ ~ 3 0 5₄ において、配信用鍵データ $K D b_1$ ~ $K D b_4$ を用いて、キーファイル K F b が復号され、権利書データ 1 0 6 b に基づいて、コンテンツファイル C F b についてのユーザからの操作に応じた購入・利用に

関する処理が行われ、その履歴が利用履歴データ 308 に記述される。

そして、SAM 305₁ ~ 305₄ から EMD サービスセンタ 302 に、利用履歴データ 308 が送信される。

EMD サービスセンタ 302 では、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301a, 301b およびサービスプロバイダ 310 の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ 152ca, 152cb, 152s を作成する。

EMD サービスセンタ 302 は、ペイメントゲートウェイ 90 を介して決済機関 91 に、決済請求権データ 152ca, 152cb, 152s を送信し、これにより、ユーザホームネットワーク 303 のユーザが決済機関 91 に支払った金銭が、コンテンツプロバイダ 301a, 301b およびサービスプロバイダ 310 の所有者に分配される。

上述したように、EMD システム 300b によれば、セキュアコンテナ 304c 内に格納されたコンテンツファイル CFa, CFb の権利書データ 106a, 106b は、コンテンツプロバイダ 301a, 301b が作成したものをそのまま用いるため、SAM 305₁ ~ 305₄ 内において、権利書データ 106a, 106b に基づいて、コンテンツファイル CFa, CFb についての権利処理がコンテンツプロバイダ 301a, 301b の意向に沿って確実に行われる。

なお、図 81 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

第 2 実施形態の第 3 変形例

図 82 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、EMD サービスセンタ 302 が決済機関 91 に対

して、コンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済を行う場合を例示したが、本発明では、例えば、図 82 に示すように、EMD サービスセンタ 302 において、利用履歴データ 308 に基づいて、コンテンツプロバイダ 301 のための決済請求権データ 152c と、サービスプロバイダ 310 のための決済請求権データ 152s とを作成し、これらをそれぞれコンテンツプロバイダ 301 およびサービスプロバイダ 310 に送信するようにしてもよい。

この場合には、コンテンツプロバイダ 301 は、決済請求権データ 152c を用いて、ペイメントゲートウェイ 90a を介して決済機関 91a に決済を行う。また、サービスプロバイダ 310 は、決済請求権データ 152s を用いて、ペイメントゲートウェイ 90b を介して決済機関 91b に決済を行う。

第 2 実施形態の第 4 変形例

図 83 は、第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、例えば現行のインターネットのようにサービスプロバイダ 310 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 310 が課金機能を有している場合には、CA モジュール 311 において、セキュアコンテナ 304 に関するサービスプロバイダ 310 のサービスに対しての利用履歴データ 308s を作成してサービスプロバイダ 310 に送信する。

そして、サービスプロバイダ 310 は、利用履歴データ 308s に基づいて、課金処理を行って決済請求権データ 152s を作成し、これを用いてペイメントゲートウェイ 90b を介して決済機関 91b に決済を行う。

一方、SAM 305₁ ~ 305₄ は、セキュアコンテナ 304 に関するコンテンツプロバイダ 301 の権利処理に対しての利用履歴データ 308c を作成し、これを EMD サービスセンタ 302 に送信する。

EMD サービスセンタ 302 は、利用履歴データ 308c に基づいて、決済請

求権データ 152c を作成し、これをコンテンツプロバイダ 301 に送信する。

コンテンツプロバイダ 301 は、決済請求権データ 152c を用いて、ペイメントゲートウェイ 90a を介して決済機関 91a に決済を行う。

第2実施形態の第5変形例

上述した実施形態では、図49に示すように、EMDサービスセンタ 302 のユーザ嗜好フィルタ生成部 901 において、SAM 305₁ などから受信した利用履歴データ 308 に基づいて、ユーザ嗜好フィルタデータ 903 を生成する場合を例示したが、例えば、図67に示す SAM 305₁ などの利用監視部 186 で生成した利用制御状態データ 166 をリアルタイムで EMD サービスセンタ 302 に送信するようにして、SP 用購入履歴データ 309 において、利用制御状態データ 166 に基づいてユーザ嗜好フィルタデータ 903 を生成するようにしてもよい。

第2実施形態の第6変形例

コンテンツプロバイダ 301、サービスプロバイダ 310 および SAM 305₁ ~ 305₄ は、それぞれ自らの公開鍵データ $K_{CP, P}$, $K_{SP, P}$, $K_{SAM1, P}$ ~ $K_{SAM4, P}$ の他に、自らの秘密鍵データ $K_{CP, S}$, $K_{SP, S}$, $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を EMD サービスセンタ 302 に登録してもよい。

このようにすることで、EMD サービスセンタ 302 は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ $K_{CP, S}$, $K_{SP, S}$, $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を用いて、コンテンツプロバイダ 301 とサービスプロバイダ 310 との間の通信、サービスプロバイダ 310 と SAM 305₁ ~ 305₄ との間の通信、並びにユーザホームネットワーク 303 内での SAM 305₁ ~ 305₄ 相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、SAM 305₁ ~ 305₄ については、出荷時に、EMD サービスセンタ 302 によって秘密鍵データ $K_{SAM1, S}$ ~ $K_{SAM4, S}$ を生成し、これを SAM 305₁ ~ 305₄ に格納すると共に EMD サービスセンタ 302 が保持（登録）す

るようにしてもよい。

第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCER_{CP}、CER_{SP}、CER_{SAM1}～CER_{SAM4}を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、相互に通信を行う場合に、EMDサービスセンタ302から事前に公開鍵証明書データCER_{CP}、CER_{SP}、CER_{SAM1}～CER_{SAM4}を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が、通信時に、EMDサービスセンタ302から公開鍵証明書データCER_{CP}、CER_{SP}、CER_{SAM1}～CER_{SAM4}を取得してもよい。

図84は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。

なお、図84において、図49と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク303aは、前述したユーザホームネットワーク303と同じである。ユーザホームネットワーク303bでは、IEEE1394シリアルバスであるバス191を介してSAM305₁₁～305₁₄を接続している。

コンテンツプロバイダ301がサービスプロバイダ310の公開鍵証明書データCER_{SP}を取得する場合には、例えば、通信に先立ってサービスプロバイダ310からコンテンツプロバイダ301に公開鍵証明書データCER_{SP}を送信する

場合（図84中（3））と、コンテンツプロバイダ301がEMDサービスセンタ302から公開鍵証明書データ CER_{SP} を取り寄せる場合（図84中（1））とがある。

また、サービスプロバイダ310がコンテンツプロバイダ301の公開鍵証明書データ CER_{CP} を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ301からサービスプロバイダ310に公開鍵証明書データ CER_{CP} を送信する場合（図84中（2））と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データ CER_{CP} を取り寄せる場合（図84中（4））とがある。

また、サービスプロバイダ310が $SAM_{305_1} \sim 305_4$ の公開鍵証明書データ $CER_{SAM_1} \sim CER_{SAM_4}$ を取得する場合には、例えば、通信に先立って $SAM_{305_1} \sim 305_4$ からサービスプロバイダ310に公開鍵証明書データ $CER_{SAM_1} \sim CER_{SAM_4}$ を送信する場合（図84中（6））と、サービスプロバイダ310がEMDサービスセンタ302から公開鍵証明書データ $CER_{SAM_1} \sim CER_{SAM_4}$ を取り寄せる場合（図84中（4））とがある。

また、 $SAM_{305_1} \sim 305_4$ がサービスプロバイダ310の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ310から $SAM_{305_1} \sim 305_4$ に公開鍵証明書データ CER_{SP} を送信する場合（図84中（5））と、 $SAM_{305_1} \sim 305_4$ がEMDサービスセンタ302から公開鍵証明書データ CER_{SP} を取り寄せる場合（図84中（7）など）とがある。

また、 SAM_{305_1} が SAM_{305_2} の公開鍵証明書データ CER_{SAM_2} を取得する場合には、例えば、通信に先立って SAM_{305_2} から SAM_{305_1} に公開鍵証明書データ CER_{SAM_2} を送信する場合（図84中（8））と、 SAM_{305_1} がEMDサービスセンタ302から公開鍵証明書データ CER_{SAM_2} を取り寄せる場合（図84中（7）など）とがある。

また、SAM305₂がSAM305₁の公開鍵証明書データCER_{SAM1}を取得する場合には、例えば、通信に先立ってSAM305₁からSAM305₂に公開鍵証明書データCER_{SAM1}を送信する場合（図84中（9））と、SAM305₂が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM1}を取り寄せる場合と、SAM305₁が搭載されたネットワーク機器を介して公開鍵証明書データCER_{SAM1}を取り寄せる場合（図84中（7），（8））とがある。

また、SAM305₄がSAM305₁₃の公開鍵証明書データCER_{SAM13}を取得する場合には、例えば、通信に先立ってSAM305₁₃からSAM305₄に公開鍵証明書データCER_{SAM13}を送信する場合（図84中（12））と、SAM305₄が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM13}を取り寄せる場合（図84中（10））と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SAM13}を取り寄せる場合とがある。

また、SAM305₁₃がSAM305₄の公開鍵証明書データCER_{SAM4}を取得する場合には、例えば、通信に先立ってSAM305₄からSAM305₁₃に公開鍵証明書データCER_{SAM4}を送信する場合（図84中（11））と、SAM305₁₃が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM4}を取り寄せる場合（図84中（13））と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SAM4}を取り寄せる場合とがある。

第2実施形態における公開鍵証明書破棄リスト（データ）の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを

作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄に送信する。

なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において生成してもよい。

まず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}を無効にする場合について説明する。

図85に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{CP}を無効にすることを示す公開鍵証明書破棄データCRL₁をサービスプロバイダ310に送信する(図85中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{CP, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に送信する(図85中(1),(2))。SAM305₁は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{CP, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₁を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図85中(3))。

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データCER_{SP}を無効にする場合について説明する。

図86に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{SP}を無効にすることを示す公開鍵証明書破棄データCRL₂をコンテンツプロバイダ301に送信する(図86中(1))。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER_{SP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SP, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に送信する(図86中(2))。SAM305₁は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データCRL₂を参照して公開鍵証明書データCER_{SP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SP, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₂は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要

がある。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₂を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図86中(3))。

次に、EMDサービスセンタ302が、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にする場合について説明する。

図87に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃をコンテンツプロバイダ301に送信する(図87中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えばSAM305₁に公開鍵証明書破棄データCRL_{SAM1}を送信する(図87中(1))。SAM305₁は、SAM305₂から入力したデータに付加されたSAM305₂の署名データを検証する際に、公開鍵証明書破棄データCRL₃を参照して公開鍵証明書データCER_{SAM2}の有効性を判断し、有効であると判断した場合に公開鍵データK_{SAM2, P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい(図87中(1),(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL_sを、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図87中(3))。

また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL_sを作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図88中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL_sによって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図88中(1))。

SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL_sを作成し、これをコンテンツプロバイダ301に送信する(図88中(2))。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL_sをサービスプロバイダ310に送信する(図88中(2))。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL_sをSAM305₁に送信する(図88中(2))。

SAM 305₁ は、自らが作成したSAM登録リストに示されるSAM 305₁ ~ 305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM 305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM 305₁ は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する（図88中（3））。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM 305₁に送信する（図88中（3））。

SAM 305₁ は、自らが作成したSAM登録リストに示されるSAM 305₁ ~ 305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM 305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM 305₁ は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

EMDサービスセンタ302の役割等

図89は、図49に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301

およびサービスプロバイダ 310 の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ 90 を介して決済機関 91 において決済を行う。

また、権利管理用クリアリングハウス 950 は、電子決済用クリアリングハウス 951 からの決済通知に応じたコンテンツプロバイダ 301 およびサービスプロバイダ 310 の決済レポートを作成し、それらをコンテンツプロバイダ 301 およびコンテンツプロバイダ 301 に送信する。

また、コンテンツプロバイダ 301 の権利書データ 106 およびコンテンツ鍵データ Kc の登録（権威化）などを行う。

なお、図 90 に示すように、権利管理用クリアリングハウス 950 と電子決済用クリアリングハウス 951 とを単体の装置内に収納すると、図 49 に示す EMD サービスセンタ 302 となる。

また、本発明は、例えば、図 91 に示すように、EMD サービスセンタ 302 に、権利管理用クリアリングハウス 960 の機能を設け、権利管理用クリアリングハウス 960 において、権利書データ 106 の登録などを行うと共に、SAM からの利用履歴データ 308 に基づいてサービスプロバイダ 310 の決済請求権データを作成し、これをサービスプロバイダ 310 に送信してもよい。この場合には、サービスプロバイダ 310 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 960 からの決済請求権データに基づいて決済を行う。

また、本発明は、例えば、図 92 に示すように、EMD サービスセンタ 302 に、権利管理用クリアリングハウス 970 の機能を設け、権利管理用クリアリングハウス 970 において、権利書データ 106 の登録などを行うと共に、SAM からの利用履歴データ 308 に基づいてコンテンツプロバイダ 301 の決済請求権データを作成し、これをコンテンツプロバイダ 301 に送信してもよい。この場合には、コンテンツプロバイダ 301 は、自らの課金システムを電子決済用クリアリングハウス 961 として利用し、権利管理用クリアリングハウス 970 か

らの決済請求権データに基づいて決済を行う。

第2実施形態の第8変形例

上述した第2実施形態では、図48に示すEMDシステム300において、コンテンツプロバイダ301からサービスプロバイダ310に図4に示すフォーマットのセキュアコンテナ104を提供し、サービスプロバイダ310からユーザホームネットワーク303に図53に示すフォーマットのセキュアコンテナ304を配給する場合を例示した。

すなわち、上述した第2実施形態では、図4および図53に示すように、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ単数のコンテンツファイルCFと、当該コンテンツファイルCFに対応する単数のキーファイルKFを格納した場合を例示した。

本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFにそれぞれ対応する複数のキーファイルKFとを格納してもよい。

図93は、本変形例において、図48に示すコンテンツプロバイダ301からサービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。

図93に示すように、セキュアコンテナ104aには、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公開鍵証明書データCER_{CP}、署名データSIG_{1, BSC}および署名データSIG_{250, CP}が格納されている。

ここで、署名データSIG_{250, CP}は、コンテンツプロバイダ301において、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公開鍵証明書データCER_{CP}および署名データSIG_{1, BSC}の全体に対してハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データK_{CP, s}を用いて生成される。

コンテンツファイル CF_{101} には、ヘッダ、リンクデータ LD_1 、メタデータ $Meta_1$ 、コンテンツデータ C_1 およびA/V伸長用ソフトウェア $Soft_1$ が格納されている。

ここで、コンテンツデータ C_1 およびA/V伸長用ソフトウェア $Soft_1$ は、前述したコンテンツ鍵データ Kc_1 を用いて暗号化されており、メタデータ $Meta_1$ は必要に応じてコンテンツ鍵データ Kc_1 を用いて暗号化されている。

また、コンテンツデータ C_1 は、例えば、ATRAC3方式で圧縮されている。A/V伸長用ソフトウェア $Soft_1$ は、ATRAC3方式の伸長用のソフトウェアである。

また、リンクデータ LD_1 は、キーファイル KF_{101} にリンクすることを示している。

コンテンツファイル CF_{102} には、ヘッダ、リンクデータ LD_1 、メタデータ $Meta_2$ 、コンテンツデータ C_2 およびA/V伸長用ソフトウェア $Soft_2$ が格納されている。

ここで、コンテンツデータ C_2 およびA/V伸長用ソフトウェア $Soft_2$ は、前述したコンテンツ鍵データ Kc_2 を用いて暗号化されており、メタデータ $Meta_2$ は必要に応じてコンテンツ鍵データ Kc_2 を用いて暗号化されている。

また、コンテンツデータ C_2 は、例えば、MPEG2方式で圧縮されている。A/V伸長用ソフトウェア $Soft_2$ は、MPEG2方式の伸長用のソフトウェアである。

また、リンクデータ LD_2 は、キーファイル KF_{102} にリンクすることを示している。

コンテンツファイル CF_{103} には、ヘッダ、リンクデータ LD_3 、メタデータ $Meta_3$ 、コンテンツデータ C_3 およびA/V伸長用ソフトウェア $Soft_3$ が格納されている。

ここで、コンテンツデータ C_3 およびA/V伸長用ソフトウェア $Soft_3$ は

、前述したコンテンツ鍵データ Kc_s を用いて暗号化されており、メタデータ $Meta_s$ は必要に応じてコンテンツ鍵データ Kc_s を用いて暗号化されている。

また、コンテンツデータ C_s は、例えば、JPEG方式で圧縮されている。A/V伸長用ソフトウェア $Soft_s$ は、JPEG方式の伸長用のソフトウェアである。

また、リンクデータ LD_s は、キーファイル KF_{10s} にリンクすることを示している。

キーファイル KF_{101} には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_s$ を用いて暗号化されたコンテンツ鍵データ Kc_1 、権利書データ 106_1 、SAMプログラム・ダウンロード・コンテナ SDC_1 および署名・証明書モジュール Mod_{200} とが格納されている。

ここで、署名・証明書モジュール Mod_{200} には、図94Aに示すように、それぞれコンテンツデータ C_1 、コンテンツ鍵データ Kc_1 および権利書データ 106_1 のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データ $K_{CP,s}$ を用いて作成した署名データ $SIG_{211,CP}$ 、 $SIG_{212,CP}$ 、 $SIG_{213,CP}$ と、公開鍵データ $K_{CP,P}$ の公開鍵証明書データ CER_{CP} と、当該公開鍵証明書データ CER_{CP} に対してのEMDサービスセンタ302の署名データ $SIG_{1,BSC}$ とが格納されている。

キーファイル KF_{102} には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_s$ を用いて暗号化されたコンテンツ鍵データ Kc_2 、権利書データ 106_2 、SAMプログラム・ダウンロード・コンテナ SDC_2 および署名・証明書モジュール Mod_{201} とが格納されている。

ここで、署名・証明書モジュール Mod_{201} には、図94Bに示すように、それぞれコンテンツデータ C_2 、コンテンツ鍵データ Kc_2 および権利書データ 106_2 のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データ $K_{CP,s}$ を用いて作成した署名データ $SIG_{221,CP}$ 、 $SIG_{222,CP}$ 、 $SIG_{223,CP}$ と、公

開鍵証明書データ CER_{CP} と、当該公開鍵証明書データ CER_{CP} に対しての署名データ $SIG_{1, BSC}$ とが格納されている。

キーファイル KF_{103} には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ K_{CS} 、権利書データ 106_s 、SAMプログラム・ダウンロード・コンテナ SDC_s および署名・証明書モジュール Mod_{202} とが格納されている。

ここで、署名・証明書モジュール Mod_{202} には、図 9 4 C に示すように、それぞれコンテンツデータ C_s 、コンテンツ鍵データ K_{CS} および権利書データ 106_s のハッシュ値をとり、コンテンツプロバイダ 3 0 1 の秘密鍵データ $K_{CP, S}$ を用いて作成した署名データ $SIG_{231, CP}$ 、 $SIG_{232, CP}$ 、 $SIG_{233, CP}$ と、公開鍵証明書データ CER_{CP} と、当該公開鍵証明書データ CER_{CP} に対しての署名データ $SIG_{1, BSC}$ とが格納されている。

サービスプロバイダ 3 1 0 は、図 9 3 に示すセキュアコンテナ 1 0 4 a の配給を受けると、EMD サービスセンタ 3 0 2 の公開鍵データ $K_{BSC, P}$ を用いて公開鍵証明書データ CER_{CP} の正当性を確認した後に、当該公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP, P}$ を用いて、署名データ $SIG_{250, CP}$ の正当性を確認する。

そして、サービスプロバイダ 3 1 0 は、署名データ $SIG_{250, CP}$ の正当性を確認すると、図 9 5 に示すように、セキュアコンテナ 1 0 4 a から得たコンテンツファイル CF_{101} 、 CF_{102} 、 CF_{103} およびキーファイル KF_{101} 、 KF_{102} 、 KF_{103} と、サービスプロバイダ 3 1 0 の公開鍵証明書データ CER_{SP} と、署名データ $SIG_{31, BSC}$ と、プライスタグデータ 312_1 、 312_2 、 312_3 と、署名データ $SIG_{280, SP}$ とを格納したセキュアコンテナ 3 0 4 a を作成する。

ここで、プライスタグデータ 312_1 、 312_2 、 312_3 は、それぞれコンテンツデータ C_1 、 C_2 、 C_3 の販売価格を示している。

また、署名データ $SIG_{280, SP}$ は、コンテンツファイル CF_{101} 、 CF_{102} 、

CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公開鍵証明書データCER_{SP}と、署名データSIG_{81, BSC}およびプライスタグデータ312₁、312₂、312₃の全体に対してハッシュ値をとり、サービスプロバイダ310の秘密鍵データK_{SP, s}を用いて生成される。

サービスプロバイダ310は、図95に示すセキュアコンテナ304aをユーザホームネットワーク303に配給する。

ユーザホームネットワーク303では、SAM305₁～305₄において、セキュアコンテナ304aに格納された署名データSIG_{81, BSC}の正当性を確認した後に、公開鍵証明書データCER_{SP}に格納された公開鍵データK_{SP, KP}を用いて、署名データSIG_{280, SP}の正当性を確認する。

その後、SAM305₁～305₄は、コンテンツデータC₁₀₁、C₁₀₂、C₁₀₃についての権利処理を、リンクデータLD₁、LD₂、LD₃に示されるリンク状態に応じて、それぞれキーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃に基づいて行う。

なお、上述した第8変形例では、コンテンツプロバイダ301において、図93に示すように、コンテンツプロバイダ301において、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公開鍵証明書データCER_{CP}および署名データSIG_{1, BSC}の全体に対しての署名データSIG_{250, CP}を作成する場合を例示したが、例えば、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃およびキーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃のそれぞれについて署名データを作成し、これをセキュアコンテナ104a内に格納してもよい。

また、上述した第8変形例では、サービスプロバイダ310において、図95に示すように、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公開鍵証明書データCER_{SP}と、署名データSIG_{81, BSC}およびプライスタグデータ312₁、312₂、312₃の全体に

対しての署名データ $SIG_{280, SP}$ を作成する場合を例示したが、これらの各々についての署名データを作成し、これらをセキュアコンテナ 304a に格納するようにしてもよい。

また、上述した第8変形例では、セキュアコンテナ 304 において、単数のサービスプロバイダ 310 から提供を受けた複数のコンテンツファイル CF_{101} , CF_{102} , CF_{103} を単数のセキュアコンテナ 304a に格納してユーザホームネットワーク 303 に配給する場合を例示したが、図81に示すように、複数のコンテンツプロバイダ 301a, 301b から提供を受けた複数のコンテンツファイル CF を、単数のセキュアコンテナに格納してユーザホームネットワーク 303 に配給してもよい。

なお、図93に示すフォーマットは、前述した第1実施形態において、図1に示すコンテンツプロバイダ 101 からユーザホームネットワーク 103 にセキュアコンテナ 104 を送信する場合にも同様に適用できる。

また、上述した実施形態では、EMDサービスセンタにおいて、SAMから入力した利用履歴データに基づいて決済処理を行う場合を例示したが、SAMにおいてコンテンツの購入形態が決定される度に利用制御状態データをSAMからEMDサービスセンタに送信し、EMDサービスセンタにおいて、受信した利用制御状態データを用いて決済処理を行ってもよい。

以下、コンテンツプロバイダ 101 において作成されるコンテンツファイル CF およびキーファイル KF などの概念をまとめる。

コンテンツプロバイダ 101 がインターネットを用いてコンテンツを提供する場合には、図96に示すように、ヘッダ、コンテンツID、コンテンツ鍵データ Kc を用いた暗号化されたコンテンツデータ C および署名データを含むコンテンツファイル CF が作成される。当該コンテンツデータ C の取り扱いを示す権利書データと、コンテンツ鍵データ Kc とが、所定の信頼機関であるEMDサービスセンタ 102, 302 の配信用鍵データによって暗号化された後に、キーファイ

ルKFに格納される。また、キーファイルKFには、ヘッダ、コンテンツID、必要に応じてメタデータ、署名データが格納される。

そして、コンテンツファイルCFおよびキーファイルKFが、コンテンツプロバイダ101からユーザホームネットワーク103, 303に直接提供されたり、コンテンツプロバイダ101からサービスプロバイダ310を介してユーザホームネットワーク103, 303に提供される。

また、コンテンツプロバイダ101がインターネットを用いてコンテンツを提供する場合に、図97に示すように、キーファイルKF内にコンテンツ鍵データKcを格納しないで、所定の信頼機関であるEMDサービスセンタ102, 302の配信用鍵データによって暗号化したコンテンツ鍵データKcをEMDサービスセンタ102, 302からユーザホームネットワーク103, 303に提供してもよい。

また、コンテンツプロバイダ101がデジタル放送を用いてコンテンツを提供する場合に、例えば、図98に示すように、コンテンツ鍵データKcを用いて暗号化したコンテンツデータCと署名データとを、コンテンツプロバイダ101からユーザホームネットワーク103, 303に、直接あるいはサービスプロバイダ310を介して提供する。この場合に、図97に示すキーファイルKFに対応する鍵データブロックを、コンテンツプロバイダ101からユーザホームネットワーク103, 303に、直接あるいはサービスプロバイダ310を介して提供する。

また、この場合に、例えば、図99に示すように、所定の信頼機関であるEMDサービスセンタ102, 302の配信用鍵データによって暗号化したコンテンツ鍵データKcをEMDサービスセンタ102, 302からユーザホームネットワーク103, 303に提供してもよい。

産業上の利用可能性

以上説明したように、本発明によれば、データ提供装置の関係者の利益が適切に保護される。

また、本発明によれば、権利書データなどが不正に改竄されることを適切に回避できる。

また、本発明によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

請求の範囲

1. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

2. 前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項1に記載のデータ提供システム。

3. 前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項2に記載のデータ提供システム。

4. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配

給する

請求項 1 に記載のデータ提供システム。

5. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 に記載のデータ提供システム。

6. 前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置

をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 5 に記載のデータ提供システム。

7. 前記データ提供装置は、

前記コンテンツデータを格納した第 1 のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第 2 のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項 1 に記載のデータ提供システム。

8. 前記データ提供装置は、前記第 1 のファイルおよび前記第 2 のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 7 に記載のデータ提供システム。

9. 前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 8 に記載のデータ提供システム。

10. 前記データ提供装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化

し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 1 に記載のデータ提供システム。

1 1. 前記データ提供装置は、前記モジュールを記録した記録媒体を作成する

請求項 1 に記載のデータ提供システム。

1 2. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項 1 に記載のデータ提供システム。

1 3. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項 1 に記載のデータ提供システム。

1 4. 前記データ処理装置は、前記モジュールに格納された公開鍵データを用いて、前記モジュールに格納された署名データの正当性を検証する

請求項 9 に記載のデータ提供システム。

1 5. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 3 に記載のデータ提供システム。

1 6. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項 1 に記載のデータ提供システム。

1 7. データ提供装置から配給されたコンテンツデータを利用するデータ処理

装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ処理装置。

18. データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

19. 前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する

請求項18に記載のデータ提供システム。

20. 前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記第1のモジュール

ルを前記データ配給装置に提供し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項18に記載のデータ提供システム。

21. 前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項20に記載のデータ提供システム。

22. 前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納し、前記配信用鍵データを用いて暗号化された第3のモジュールを格納した前記第1のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第3のモジュールを前記第2のモジュールに格納して前記データ処理装置に配給する

請求項20に記載のデータ提供システム。

23. 前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記第3のモジュールを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項22に記載のデータ提供システム。

24. 前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置

をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記第3のモジュールを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項23に記載のデータ提供システム。

25. 前記データ提供装置は、

前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項18に記載のデータ提供システム。

26. 前記データ提供装置は、前記第1のファイルおよび前記第2のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項25に記載のデータ提供システム。

27. 前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項25に記載のデータ提供システム。

28. 前記データ配給装置は、前記価格データに対して自らの秘密鍵データを用いて署名データを作成し、当該署名データを前記第2のモジュールに格納して前記データ処理装置に配給する

請求項19に記載のデータ提供システム。

29. 前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記第2のモジュールを前記データ処理装置に提供する

請求項28に記載のデータ提供システム。

30. 前記データ配給装置は、前記第1のファイルおよび前記第2のファイルについての署名データを、前記データ提供装置の公開鍵データを用いて検証する

請求項26に記載のデータ提供システム。

31. 前記データ提供装置は、

前記第1のファイルと、第2のファイルとのリンク関係を示すリンクデータを格納した前記第1のモジュールを前記データ配給装置に提供する

請求項 2 5 に記載のデータ提供システム。

3 2. 前記データ配給装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記第 2 のモジュールを暗号化し、当該暗号化した第 2 のモジュールを前記データ処理装置に送信する

請求項 1 8 に記載のデータ提供システム。

3 3. 前記データ配給装置は、前記モジュールを記録した記録媒体を作成する
請求項 1 8 に記載のデータ提供システム。

3 4. 前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項 1 8 に記載のデータ提供システム。

3 5. 前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項 1 8 に記載のデータ提供システム。

3 6. 前記データ処理装置は、前記第 2 のモジュールに格納された公開鍵データを用いて、前記第 2 のモジュールに格納された署名データの正当性を検証する

請求項 2 9 に記載のデータ提供システム。

3 7. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 2 1 に記載のデータ提供システム。

3 8. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定の

データおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項 18 に記載のデータ提供システム。

39. データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記複数のデータ配給装置に提供し、

前記第1のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを前記データ処理装置に配給し、

前記第2のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

40. 少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記第1のデータ提供装置は、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、

前記第 2 のデータ提供装置は、第 2 のコンテンツ鍵データを用いて暗号化された第 2 のコンテンツデータと、暗号化された前記第 2 のコンテンツ鍵データと、前記第 2 のコンテンツデータの取り扱いを示す暗号化された第 2 の権利書データとを格納した第 2 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化された前記第 1 のコンテンツデータ、前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データと、前記提供を受けた前記第 2 のモジュールに格納された前記暗号化された前記第 2 のコンテンツデータ、前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データとを格納した第 3 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 3 のモジュールに格納された前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データを復号し、当該復号した第 1 の権利書データに基づいて、前記第 1 のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第 3 のモジュールに格納された前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データを復号し、当該復号した第 2 の権利書データに基づいて、前記第 2 のコンテンツデータの取り扱いを決定する

データ提供システム。

4 1. コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供装置。

4 2. 前記権利書データを作成、当該作成した権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

4 3. 配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

4 4. 所定の権威機関が発行した前記配信用鍵データを用いて、前記コンテンツ鍵データ K c および前記権利書データを暗号化する

請求項 4 3 に記載のデータ提供装置。

4 5. 前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

4 6. 自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 5 に記載のデータ提供装置。

4 7. 前記公開鍵データの正当性を証明する公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 6 に記載のデータ提供装置。

4 8. 前記コンテンツデータを格納した第 1 のファイルと、
前記コンテンツ鍵データおよび前記権利書データを格納した第 2 のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

4 9. 前記第 1 のファイルおよび前記第 2 のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 8 に記載のデータ提供装置。

5 0. 前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 9 に記載のデータ提供装置。

5 1. 前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 4 1 に記載のデータ提供装置。

5 2. 前記モジュールを記録した記録媒体を作成する

請求項 4 1 に記載のデータ提供装置。

5 3. 前記モジュールをアプリケーション層で定義する

請求項 4 1 に記載のデータ提供装置。

5 4. 前記モジュールを前記データ処理装置に配給する配送プロトコルとして、前記アプリケーション層の下層のプレゼンテーション層およびトランスポート層を用いる

請求項 5 3 に記載のデータ提供装置。

5 5. 前記モジュールを前記データ処理装置に配給するための媒体に依存しない形式で前記モジュールを定義する

請求項 4 1 に記載のデータ提供装置。

5 6. データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納

された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

57. 前記データ提供装置から前記データ処理装置に、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項56に記載のデータ提供方法。

58. データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

59. 前記データ配給装置から前記データ処理装置に、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを配給する

請求項58に記載のデータ提供方法。

60. データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記第1のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記第2のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

61. 少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記第1のデータ提供装置から前記データ配給装置に、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを提供し、

前記第2のデータ提供装置から前記データ配給装置に、第2のコンテンツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗

号化された第 2 の権利書データとを格納した第 2 のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化された前記第 1 のコンテンツデータ、前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データと、前記提供を受けた前記第 2 のモジュールに格納された前記暗号化された前記第 2 のコンテンツデータ、前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データとを格納した第 3 のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第 3 のモジュールに格納された前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データを復号し、当該復号した第 1 の権利書データに基づいて、前記第 1 のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第 3 のモジュールに格納された前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データを復号し、当該復号した第 2 の権利書データに基づいて、前記第 2 のコンテンツデータの取り扱いを決定する

データ提供方法。

6 2. コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供方法。

6 3. 配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 2 に記載のデータ提供方法。

6 4. 前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書デー

タの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 2 に記載のデータ提供方法。

6 5. 自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 4 に記載のデータ提供方法。

6 6. 前記公開鍵データの正当性を証明する公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 5 に記載のデータ提供方法。

6 7. 前記コンテンツデータを格納した第 1 のファイルと、
前記コンテンツ鍵データおよび前記権利書データを格納した第 2 のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 2 に記載のデータ提供方法。

6 8. 前記第 1 のファイルおよび前記第 2 のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 7 に記載のデータ提供方法。

6 9. 前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 6 8 に記載のデータ提供方法。

7 0. 前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 6 2 に記載のデータ提供方法。

7 1. 前記モジュールを記録した記録媒体を作成する

請求項 6 2 に記載のデータ提供方法。

7 2. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

データ提供システム。

7 3. 前記データ提供装置は、前記権利書データと、自らの識別子と、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 7 2 に記載のデータ提供システム。

7 4. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給し、

前記データ提供装置は、前記公開鍵証明書データと、前記権利書データと、自らの識別子と、前記署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 7 3 に記載のデータ提供システム。

7 5. 前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成

した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記データ提供装置から受信した前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う

請求項 7 2 に記載のデータ提供システム。

7 6. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 7 2 に記載のデータ提供システム。

7 7. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを前記データ処理装置に配給し、前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ処理装置は、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理

し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

データ提供システム。

78. 前記データ提供装置は、前記コンテンツデータおよび前記コンテンツ鍵データを格納したモジュールを、前記データ処理装置に配給する

請求項77に記載のデータ提供システム。

79. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

管理装置。

80. 前記データ提供装置から、前記権利書データと、当該データ提供装置の識別子と、少なくとも前記権利書データに対して当該データ提供装置の秘密鍵データを用いて作成した署名データとを格納したモジュールを用いた前記要求を受けける場合に、

前記データ提供装置の秘密鍵データに対応する公開鍵データを管理する請求項79に記載の管理装置。

81. 前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ提供装置に送信する

請求項80に記載の管理装置。

82. コンテンツ鍵データを用いて暗号化したコンテンツデータ、および当該コンテンツデータの取り扱いを示す権利書データを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータを前記コンテンツ鍵データを用いて復号した後に当該コンテンツデータの利用

を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

管理装置。

8 3. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記権利書データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

データ提供システム。

8 4. 前記データ提供装置は、前記コンテンツデータの識別子と、前記権利書データと、少なくとも前記権利書データに対して自らの秘密鍵データを用いて作成した署名データとを格納したモジュールを前記管理装置に送信して前記要求を行う

請求項 8 3 に記載のデータ提供システム。

8 5. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを、自らの秘密鍵データを用いて作成した署名データと共に、前記データ提供装置に配給する

請求項 8 4 に記載のデータ提供システム。

86. 前記管理装置は、配信鍵データを管理し、当該配信鍵データを前記データ処理装置に配給し、前記データ提供装置からの要求に応じて、前記権利書データに対して自らの秘密鍵データを用いて作成した署名データを生成し、当該生成した署名データと前記権利書データとを格納したモジュールを前記配信鍵データを用いて暗号化して前記データ提供装置に送信し、

前記データ提供装置は、前記管理装置から受信したモジュールを前記データ配給装置に提供し、

前記データ処理装置は、前記データ配給装置から配給を受けた前記モジュールを、前記配信鍵データを用いて復号し、当該モジュールに格納された前記署名データの正当性を前記管理装置の公開鍵データを用いて検証し、正当であると判断した場合に、前記モジュールに格納された権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行う

請求項83に記載のデータ提供システム。

87. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する

請求項83に記載のデータ提供システム。

88. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 8 3 に記載のデータ提供システム。

8 9. 前記データ処理装置は、前記データ配給装置と通信を行う第 1 のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第 2 のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第 2 のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 8 3 に記載のデータ提供システム。

9 0. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、前記コンテンツ鍵データおよび前記コンテンツ鍵データの正当性を証明することを前記管理装置に要求し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理

し、前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

データ提供システム。

9 1. 前記データ提供装置は、前記コンテンツ鍵データを暗号化し、当該暗号化したコンテンツ鍵データと前記暗号化したコンテンツデータとを格納したモジュールを前記データ配給装置に提供する

請求項 9 0 に記載のデータ提供システム。

9 2. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行うデータ処理装置とを管理する管理装置であって、

前記データ提供装置からの要求に応じて、前記権利書データの正当性を証明する

管理装置。

9 3. 前記コンテンツデータをコンテンツ鍵データを用いて暗号化して前記データ提供装置から前記データ配給装置に提供する場合に、

前記データ提供装置からの要求に応じて、前記コンテンツ鍵データの正当性を証明する

請求項 9 2 に記載の管理装置。

9 4. 前記価格データを前記コンテンツデータおよび前記権利書データと共に、前記データ配給装置から前記データ処理装置に配給する場合に、

前記データ配給装置からの要求に応じて、前記価格データの正当性を証明する

請求項 9 2 に記載の管理装置。

9 5. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において前記権利書データの正当性を証明する

データ提供方法。

96. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータを配給し、

前記データ処理装置において、前記配給を受けたコンテンツデータを、前記コンテンツ鍵データを用いて復号し、当該復号したコンテンツデータを利用し、

前記データ提供装置からの要求に応じて、前記管理装置において前記コンテンツ鍵データの正当性を証明する

データ提供方法。

97. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記権利書

データの正当性を証明する

データ提供方法。

98. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化したコンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて、前記コンテンツ鍵データを用いた前記コンテンツデータの復号を含む前記コンテンツデータの利用を行い、

前記データ提供装置からの要求に応じて、前記管理装置において、前記コンテンツ鍵データの正当性を証明する

データ提供方法。

99. データ提供装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、前記データ提供装置および前記データ処理装置を管理し、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提

供装置の関係者に分配するための利益分配処理を行う

データ提供システム。

100. 前記データ提供装置は、所定の鍵データを用いて前記コンテンツデータを暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記鍵データを用いて、前記受信したコンテンツデータを復号し、

前記管理装置は、前記鍵データを管理する

請求項99に記載のデータ提供システム。

101. 前記データ提供装置は、所定の鍵データを生成し、当該生成した鍵データを前記管理装置に登録し、

前記管理装置は、前記登録された前記鍵データを管理し、前記データ処理装置において、前記コンテンツデータの購入処理が行われたときに、対応する前記鍵データを前記データ処理装置に送信し、

前記データ処理装置は、受信した前記鍵データを用いて、前記受信したコンテンツデータを復号する

請求項99に記載のデータ提供システム。

102. 前記データ提供装置は、前記鍵データを暗号化し、当該暗号化した鍵データと前記暗号化したコンテンツデータと前記権利書データとを格納したモジュールを前記データ処理装置に配給する

請求項100に記載のデータ提供システム。

103. 前記管理装置は、配信用鍵データを管理し、前記配信用鍵データを前記データ提供装置および前記データ処理装置に配給し、

前記データ提供装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを暗号化し、

前記データ処理装置は、前記配信された前記配信用鍵データを用いて前記鍵データおよび前記権利書データを復号する

請求項 1 0 2 に記載のデータ提供システム。

1 0 4. 前記管理装置は、各々所定の有効期限を持つ複数の前記配信用鍵データを、所定の期間分だけ、前記データ提供装置および前記データ処理装置に配給する

請求項 1 0 3 に記載のデータ提供システム。

1 0 5. 前記データ提供装置は、前記暗号化したコンテンツデータおよび前記権利書データの少なくとも一方に対しての署名データを自らの秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化した前記鍵データ、前記暗号化された前記権利書データおよび前記署名データを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュール内に格納された前記署名データを、前記秘密鍵データに対応する公開鍵データを用いて検証し、

前記管理装置は、前記公開鍵データを管理する

請求項 1 0 2 に記載のデータ提供システム。

1 0 6. 前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 1 0 5 に記載のデータ提供システム。

1 0 7. 前記管理装置は、前記データ提供装置の前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 1 0 5 に記載のデータ提供システム。

1 0 8. 前記管理装置は、前記データ提供装置および前記データ処理装置に、それぞれ配信鍵データを配給し、

前記データ提供装置は、前記権利書データを、前記配信鍵データを用いて暗号化して前記データ処理装置に配給し、

前記データ処理装置は、前記配信鍵データを用いて、受信した前記権利

書データを復号する

請求項 98 に記載のデータ提供システム。

109. 前記管理装置は、前記権利書データおよび前記鍵データの少なくとも一方の正当性を認証する

請求項 100 に記載のデータ提供システム。

110. 前記管理装置は、前記利益分配処理に応じた決済処理を行うことを請求する際に用いられる決済請求権データを生成し、当該決済請求権データに自らの秘密鍵データによる署名データを付加して、前記決済処理を行う装置あるいは前記データ提供装置に送信する

請求項 98 に記載のデータ提供システム。

111. 前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う

請求項 98 に記載のデータ提供システム。

112. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態を決定し、当該決定した購入形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する

請求項 98 に記載のデータ提供システム。

113. 前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである

請求項 98 に記載のデータ提供システム。

114. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを配給するデータ提供装置と、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一

方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、

前記履歴データを前記データ処理装置から受信し、当該受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を行う

管理装置。

1 1 5. 所定の鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する

請求項 1 1 3 に記載の管理装置。

1 1 6. 前記権利書データと、前記コンテンツデータを前記暗号化する際に用いる鍵データとの少なくとも一方の正当性を認証する

請求項 1 1 4 に記載の管理装置。

1 1 7. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの配給をデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記履歴データを前記管理装置に送信するデータ処理装置。

1 1 8. 前記コンテンツデータが所定の鍵データを用いて暗号化されている場合に、前記鍵データを前記データ提供装置から受ける

請求項 1 1 7 に記載のデータ処理装置。

119. 処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを用いて構成される

請求項117に記載のデータ処理装置。

120. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

データ提供システム。

121. 前記データ提供装置は、前記コンテンツデータを、コンテンツ鍵データを用いて暗号化して前記データ配給装置に提供する

請求項120に記載のデータ提供システム。

122. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを作成し、当該価格データを前記データ処理装置に配給する

請求項 1 2 0 に記載のデータ提供システム。

1 2 3. 前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを、配信鍵データを用いて暗号化して前記データ配給装置に提供し、

前記データ処理装置は、前記配信鍵データを用いて、前記コンテンツ鍵データおよび前記権利書データを復号し、

前記管理装置は、前記配信鍵データを管理し、前記配信鍵データを前記データ提供装置および前記データ処理装置に配給する

請求項 1 2 1 に記載のデータ提供システム。

1 2 4. 前記データ提供装置は、前記暗号化されたコンテンツデータ、前記暗号化されたコンテンツ鍵データおよび前記暗号化された前記権利書データの少なくとも一つのデータに対しての第 1 の署名データを自らの第 1 の秘密鍵データを用いて生成し、前記暗号化されたコンテンツデータ、前記暗号化された鍵データ、前記暗号化された権利書データおよび前記第 1 の署名データを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第 1 の秘密鍵データに対応する第 1 の公開鍵データを用いて前記第 1 の署名データを検証した後に、自らの第 2 の秘密鍵データを用いて生成した第 2 の署名データを前記第 1 のモジュールに格納して第 2 のモジュールを生成し、当該第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記第 1 の公開鍵データを用いて、前記配給を受けた前記第 2 のモジュールに格納された前記第 1 の署名データを検証し、前記第 2 の秘密鍵データに対応する第 2 の公開鍵データを用いて、前記配給を受けた前記第 2 のモジュールに格納された前記第 2 の署名データを検証し、

前記管理装置は、前記第 1 の公開鍵データおよび前記第 2 の公開鍵データを管理する

請求項 1 2 3 に記載のデータ提供システム。

1 2 5. 前記データ提供装置は、前記第 1 の公開鍵データを格納した前記第 1 の

モジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記第 1 の公開鍵データおよび前記第 2 の公開鍵データを格納した前記第 2 のモジュールを前記データ処理装置に配給する

請求項 1 2 4 に記載のデータ提供システム。

1 2 6. 前記管理装置は、前記第 1 の公開鍵データおよび前記第 2 の公開鍵データを、前記データ処理装置に配給する

請求項 1 2 4 に記載のデータ提供システム。

1 2 7. 前記データ配給装置は、前記配給するコンテンツデータの価格を示す価格データを前記データ処理装置に配給し、

前記管理装置は、前記権利書データ、前記コンテンツデータを前記暗号化する際に用いる鍵データおよび前記価格データのうち少なくとも一つのデータの正当性を認証する

請求項 1 2 0 に記載のデータ提供システム。

1 2 8. 前記データ配給装置は、前記提供された暗号化されたコンテンツデータ、前記提供された権利書データ、前記コンテンツデータを暗号化した前記鍵データおよび前記配給されたコンテンツデータの価格を示す価格データとを格納したモジュールを、前記データ処理装置に配給する

請求項 1 2 0 に記載のデータ提供システム。

1 2 9. 前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記決済処理を行う装置に送信する

請求項 1 2 0 に記載のデータ提供システム。

1 3 0. 前記管理装置は、前記利益分配処理の結果を示す決済レポートデータを

、前記データ提供装置および前記データ配給装置の少なくとも一方に送信する
請求項 1 2 9 に記載のデータ提供システム。

1 3 1. 前記管理装置は、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行って、決済を請求する際に用いられる決済請求権データを作成し、前記決済請求権データに自らの署名データを付加して、前記データ提供装置および前記サービス提供装置の少なくとも一方に送信する
請求項 1 2 0 に記載のデータ提供システム。

1 3 2. 前記管理装置は、前記データ処理装置の登録処理を行い、登録された前記データ処理装置を管理し、前記登録された前記データ処理装置から受信した前記履歴データに基づいて前記利益分配処理を行う
請求項 1 2 0 に記載のデータ提供システム。

1 3 3. 前記データ処理装置は、前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態に応じた利用制御状態データを生成し、前記利用制御状態データに基づいて、前記配給を受けたコンテンツデータの利用を制御する
請求項 1 2 0 に記載のデータ提供システム。

1 3 4. 前記データ処理装置の前記第 2 のモジュールは、その処理内容、予め内部に記憶されたデータおよび処理中のデータを、外部から監視および改竄困難なモジュールである
請求項 1 2 0 に記載のデータ提供システム。

1 3 5. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとを提供するデータ提供装置と、前記提供を受けた前記コンテンツデータおよび前記権利書データを配給するデータ配給装置と、前記配給を受けた前記権利書

データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを生成するデータ処理装置とを管理する管理装置であって、

受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

管理装置。

136. 所定のコンテンツ鍵データを用いて暗号化した前記コンテンツデータを、前記データ提供装置から前記データ処理装置に配給する場合に、

前記鍵データを管理する

請求項135に記載の管理装置。

137. 前記権利書データおよび前記コンテンツ鍵データの少なくとも一方の正当性を認証する

請求項136に記載の管理装置。

138. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書データとの提供をデータ提供装置から受けたデータ配給装置から、前記コンテンツデータおよび前記権利書データの配給を受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を所定の履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置と通信を行う第1のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信す

る第2のモジュールと

を有するデータ処理装置。

139. 処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項138に記載のデータ処理装置。

140. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行い、

前記データ処理装置は、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配する利益分配処理を行う

データ提供システム。

141. コンテンツデータと当該コンテンツデータの取り扱いを示す権利書デー

タとの配給をデータ配給装置を介してデータ提供装置から受け、当該配給を受けた前記コンテンツデータの購入および利用に伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を前記管理装置用履歴データに基づいて行う管理装置に前記履歴データを送信するデータ処理装置であって、

前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信する第1のモジュールと、

前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す前記管理装置用履歴データを前記管理装置に送信する第2のモジュールと

を有するデータ処理装置。

142. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する

データ提供システム。

143. 前記データ提供装置は、前記コンテンツデータの取り扱いを示す権利書データを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを、前記配給を受けた前記権利書データに基づいて利用し、

前記管理装置は、ルート認証局に対して階層的に下に存在するサブ認証局の役割を果たし、登録された前記データ提供装置、前記データ配給装置および前記データ処理装置で用いられる秘密鍵データに対応する公開鍵データの正当性を証明する際に用いられる公開鍵証明書データの作成および管理と、前記権利書データの認証および前記コンテンツデータに関する権利処理とを行う

請求項 1 4 2 に記載のデータ提供システム。

1 4 4. 前記データ提供装置は、前記鍵データを用いて暗号化して前記データ配給装置に提供し、

前記管理装置は、前記鍵データを管理する

請求項 1 4 3 に記載のデータ提供システム。

1 4 5. 前記データ提供装置および前記データ配給装置の各々は、他の装置との間で認証を行う際に用いられる自らの秘密鍵データを作成し、当該作成した秘密鍵データを管理し、当該秘密鍵データに対応する公開鍵データを作成し、当該公開鍵データと身分証明書および決済口座を前記管理装置に登録し、

前記管理装置は、前記登録に応じて、前記公開鍵データの正当性を証明する公開鍵証明書データを作成する

請求項 1 4 3 に記載のデータ提供システム。

1 4 6. 前記管理装置は、前記登録に応じて、前記データ提供装置および前記データ配給装置に識別番号をそれぞれ割り振り、前記データ提供装置および前記データ配給装置に、ルート認証局の公開鍵データおよび管理装置の公開鍵データを送信する

請求項 1 4 5 に記載のデータ提供システム。

147. 前記データ提供装置および前記データ配給装置の各々は、前記秘密鍵データをさらに前記管理装置に登録する

請求項145に記載のデータ提供システム。

148. 前記データ処理装置には、前記管理装置が生成した秘密鍵データおよび当該秘密鍵データに対応する公開鍵データが予め格納されている

請求項143に記載のデータ提供システム。

149. 前記データ処理装置には、前記管理装置が生成した前記公開鍵データの正当性を証明する公開鍵証明書データが予め格納されている

請求項148に記載のデータ提供システム。

150. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行う

データ提供システム。

151. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する

データ提供システム。

1 5 2. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理する

データ提供システムにおいて、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する

データ提供システム。

153. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記

データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する

データ提供システム。

154. 前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する

請求項153に記載のデータ提供システム。

155. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

156. 前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に直接配給する

請求項155に記載のデータ提供システム。

157. 前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項155に記載のデータ提供システム。

158. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効に

する公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御する

データ提供システム。

159. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御する

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けたコンテンツデータを利用する

データ提供システム。

160. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

161. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項160に記載のデータ提供システム。

162. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処

理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項 1 6 0 に記載のデータ提供システム。

1 6 3. 前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項 1 6 0 に記載のデータ提供システム。

1 6 4. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

165. データ提供装置、データ配給装置、データ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供システム。

166. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供システム。

167. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項166に記載のデータ提供システム。

168. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項166に記載のデータ提供システム。

169. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給された公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供システム。

170. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項169に記載のデータ提供システム。

171. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項 1 6 9 に記載のデータ提供システム。

1 7 2. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給する

データ提供システム。

1 7 3. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記

データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供システム。

174. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を有し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供

し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供システム。

175. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処

理を行い、当該利益分配処理の結果に基づいて決済を行う決済機能と、前記権利書データの登録を行う権利管理機能とを有する

データ提供システム。

176. 前記管理装置は、

前記決済機能を有する第1の管理装置と、

前記権利管理機能を有する第2の管理装置と

を有する

請求項175に記載のデータ提供システム。

177. 前記決済は、電子決済である

請求項175に記載のデータ提供システム。

178. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コ

コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ配給装置に供給する決済請求権データ生成機能と、前記権利書データの登録を行う権利管理機能とを有する

データ提供システム。

179. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記データ提供装置は、前記管理装置から配給を受けた決済請求権データを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置と通信を行う第1のモジュールと、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信する第2のモジュールとを有し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給する決済請求権データ生成機能

と、前記権利書データの登録を行う権利管理機能とを有する

データ提供システム。

180. データ提供装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを配給し、

前記データ処理装置において、前記配給を受けた権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

データ提供方法。

181. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを配給し、

前記データ処理装置において、前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置において、前記第2のモジュールから受信した前記履歴デ

ータに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

データ提供方法。

182. データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを提供し、

前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

前記データ処理装置において、前記データ配給装置から配給を受けた前記コンテンツデータが購入された履歴を示すデータ配給装置用購入履歴データを生成して前記データ配給装置に送信し、前記配給を受けた前記権利書データに基づいて、前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す管理装置用履歴データを前記管理装置に送信し、

前記管理装置において、前記管理装置用履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴った得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配し、

前記データ配給装置において、前記データ処理装置から受信したデータ配給装置用購入履歴データに基づいて、前記コンテンツデータの配給に関する課金処理を行う

データ提供方法。

183. データ提供装置、データ配給装置、データ処理装置および管理装置を用

いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理する

データ提供方法において、

前記データ提供装置、前記データ配給装置、前記データ処理装置および前記管理装置との間でのデータの伝送を、公開鍵暗号化方式を用いた相互認証、署名生成、署名検証と、共通鍵暗号化方式によるデータの暗号化とを用いて行うデータ提供方法。

184. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを

自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う前に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記他の装置に送信する

データ提供方法。

185. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、

前記データ提供装置、前記データ配給装置および前記データ処理装置は、他の装置との間で通信を行う際に、前記管理装置から自らの前記公開鍵証明書データを取得し、当該取得した公開鍵証明書データを前記通信時に前記他の装置に送信する

データ提供方法。

186. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツデータを利用し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置、前記データ配給装置および前記データ処理装置の各々が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置からデータの供給を受けたときに、当該データに対応する署名データの正当性を当該他の装置の公開鍵データを用いて検証する場合に、前記データ提供装置、前記データ配給装置および前記データ処理装置のそれぞれの秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、前記データ提供装置、前記データ配給装置および前記データ処理装置が前記公開鍵証明書破棄データが特定する公開鍵証明書データを用いた前記通信または前記配給を行うことを規制する

データ提供方法。

187. 前記管理装置は、不正行為に用いられた前記データ提供装置、前記データ配給装置および前記データ処理装置に対応する公開鍵証明書データを特定する前記公開鍵証明書破棄データを生成する

請求項186に記載のデータ提供方法。

188. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ提供装置は、コンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

189. 前記管理装置は、前記公開鍵証明書破棄データを前記データ処理装置に

直接配給する

請求項 1 8 8 に記載のデータ提供方法。

1 9 0. 前記管理装置は、前記公開鍵証明書破棄データを、前記データ配給装置を介して、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項 1 8 8 に記載のデータ提供方法。

1 9 1. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ提供装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ提供装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ配給装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、前記提供を受けたコンテンツデータを提供した前記データ提供装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記提供されたコンテンツデータの前記データ処理装置への配給を制御する

データ提供方法。

1 9 2. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置

が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記管理装置から前記配給を受けた公開鍵証明書破棄データに基づいて、コンテンツデータの提供先のデータ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記データ配給装置への前記コンテンツデータの提供を制御し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けたコンテンツデータを利用するデータ提供方法。

193. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータの提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給を受けた公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

194. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項193に記載のデータ提供方法。

195. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項193に記載のデータ提供方法。

196. 前記データ配給装置は、前記公開鍵証明書破棄データを、放送あるいはオンデマンド方式で前記データ処理装置に配給する

請求項160に記載のデータ提供方法。

197. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成された

ことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

198. データ提供装置、データ配給装置、データ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ配給装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ配給装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、前記配給を受けたコンテンツデータを配給した前記データ配給装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて、前記配給を受けたコンテンツデータの利用を制御する

データ提供方法。

199. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であ

るか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供方法。

200. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項199に記載のデータ提供方法。

201. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ提供装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項199に記載のデータ提供方法。

202. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データが自らによって作成されたことを示す署名データを自らの秘密鍵データを用いて作成し、他の装置が当該署名データの正当性を前記秘密鍵データに対応する公開鍵データを用いて検証する場合に、前記データ処理装置の秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータと、前記配給

された公開鍵証明書破棄データとを前記データ処理装置に配給し、

前記データ処理装置は、前記データ配給装置から配給を受けた公開鍵証明書破棄データに基づいて他のデータ処理装置の公開鍵証明書データが無効であるか否かを検証し、当該検証の結果に基づいて前記他のデータ処理装置との間の通信を制御する

データ提供方法。

203. 前記データ配給装置は、前記管理装置から配給を受けた前記公開鍵証明書破棄データを改竄困難な構成を有している

請求項202に記載のデータ提供方法。

204. 前記管理装置は、前記公開鍵証明書破棄データを配信用鍵データを用いて暗号化して前記データ配給装置に配給し、前記配信用鍵データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データを前記配信用鍵データを用いて復号する

請求項202に記載のデータ提供方法。

205. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記データ処理装置は、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データを前記管理装置に供給し、前記管理装置から供給された登録データ内の破棄フラグを参照して、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公

公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを記憶し、当該公開鍵証明書破棄データに基づいて、前記データ処理装置から供給を受けた前記登録データ内の前記破棄フラグを設定して新たな登録データを生成し、当該生成した登録データを前記データ処理装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給する

データ提供方法。

206. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ提供装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータおよび前記公開鍵証明書破棄データを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前

記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供方法。

207. データ提供装置、データ配給装置、複数のデータ処理装置および管理装置を用いてコンテンツデータの提供を行うデータ提供方法であって、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置によるデータ提供サービスの運用を管理し、前記データ処理装置が、他の装置にデータを供給するときに、当該データの正当性を示す署名データを自らの秘密鍵データを用いて作成する場合に、前記秘密鍵データに対応する公開鍵データの公開鍵証明書データを作成および管理し、前記作成した公開鍵証明書データのうち無効にする公開鍵証明書データを特定する公開鍵証明書破棄データを生成し、当該公開鍵証明書破棄データを前記データ配給装置に配給し、

前記データ提供装置は、前記データ配給装置にコンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記公開鍵証明書破棄データを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた公開鍵証明書破棄データに基づいて、自らが接続された所定のネットワーク内に接続された既に登録された前記データ処理装置を示す登録データ内の破棄フラグを設定し、当該破棄フラグによって無効であることが示された公開鍵証明書データを持つ他のデータ処理装置との間の通信を規制する

データ提供方法。

208. データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供方法において、

前記データ提供装置は、前記管理装置から配給を受けた決済請求権デー

タを用いて決済処理を行う課金機能を有し、コンテンツデータと、当該コンテンツデータの取り扱いを示す権利書データとを前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータおよび前記権利書データを前記データ処理装置に配給し、

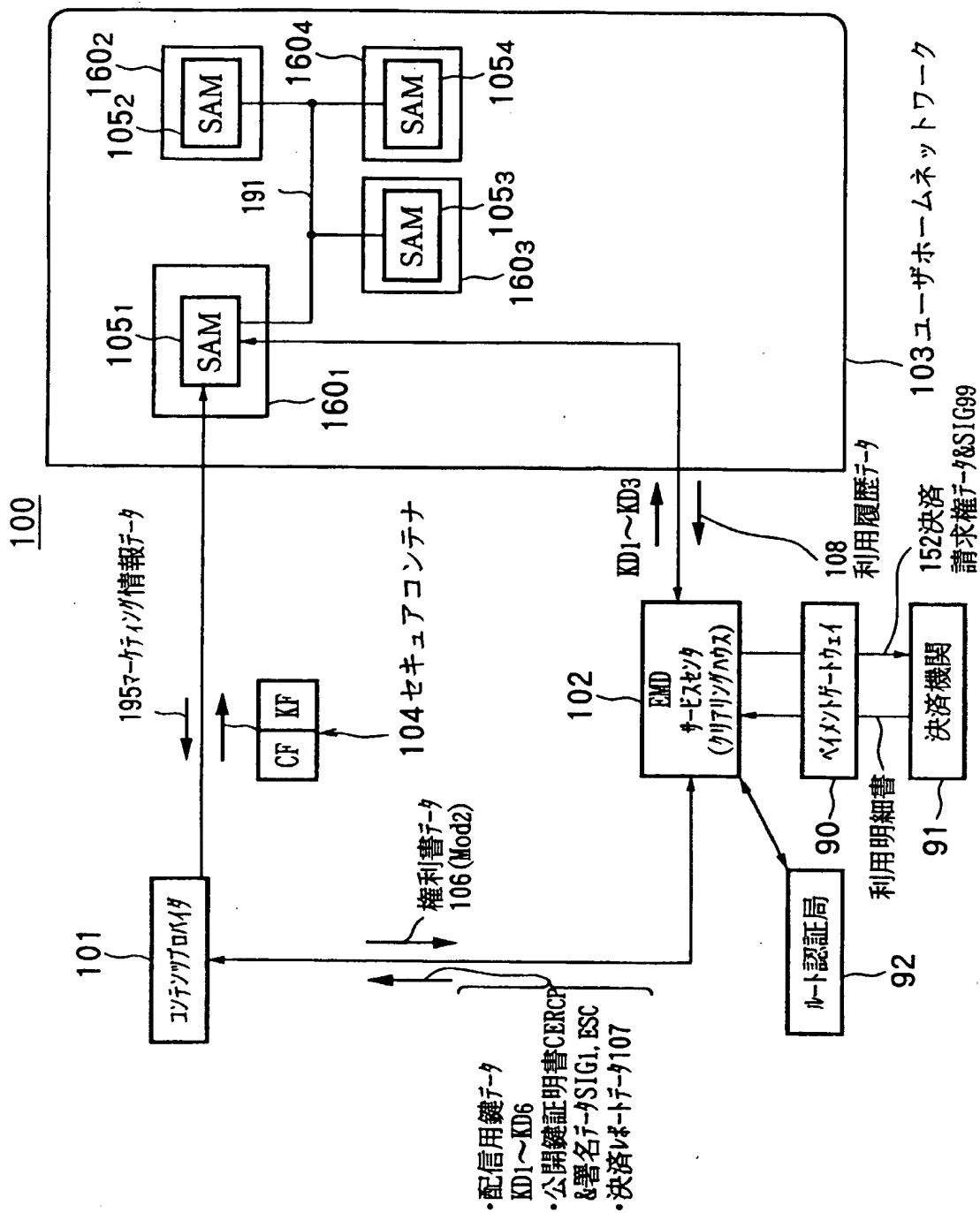
前記データ処理装置は、第1のモジュールによって前記データ配給装置と通信を行い、第2のモジュールによって前記配給を受けた前記権利書データに基づいて前記配給を受けた前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、データ提供装置、データ配給装置およびデータ処理装置を管理し、

前記第2のモジュールから受信した前記履歴データに基づいて、前記データ処理装置が前記コンテンツデータの前記配給を受けたこと、および、前記コンテンツデータを前記購入および前記利用したことに伴って得られた利益を前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行い、当該利益分配処理の結果に基づいて決済を行う際に用いられる決済請求権データを生成して前記データ提供装置に配給し、前記権利書データの登録を行う

データ提供方法。

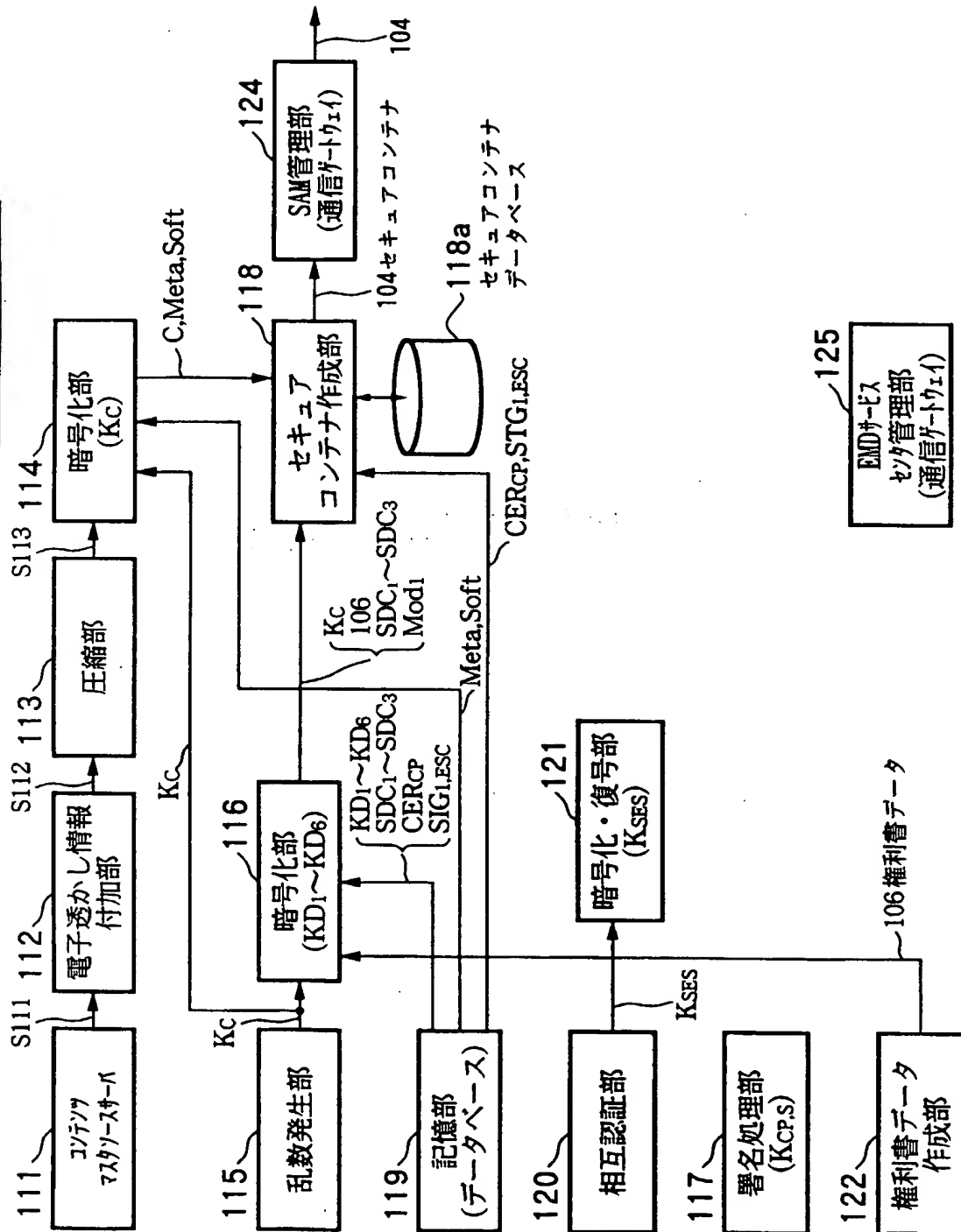
FIG. 1



THIS PAGE BLANK (USPTO)

FIG. 2

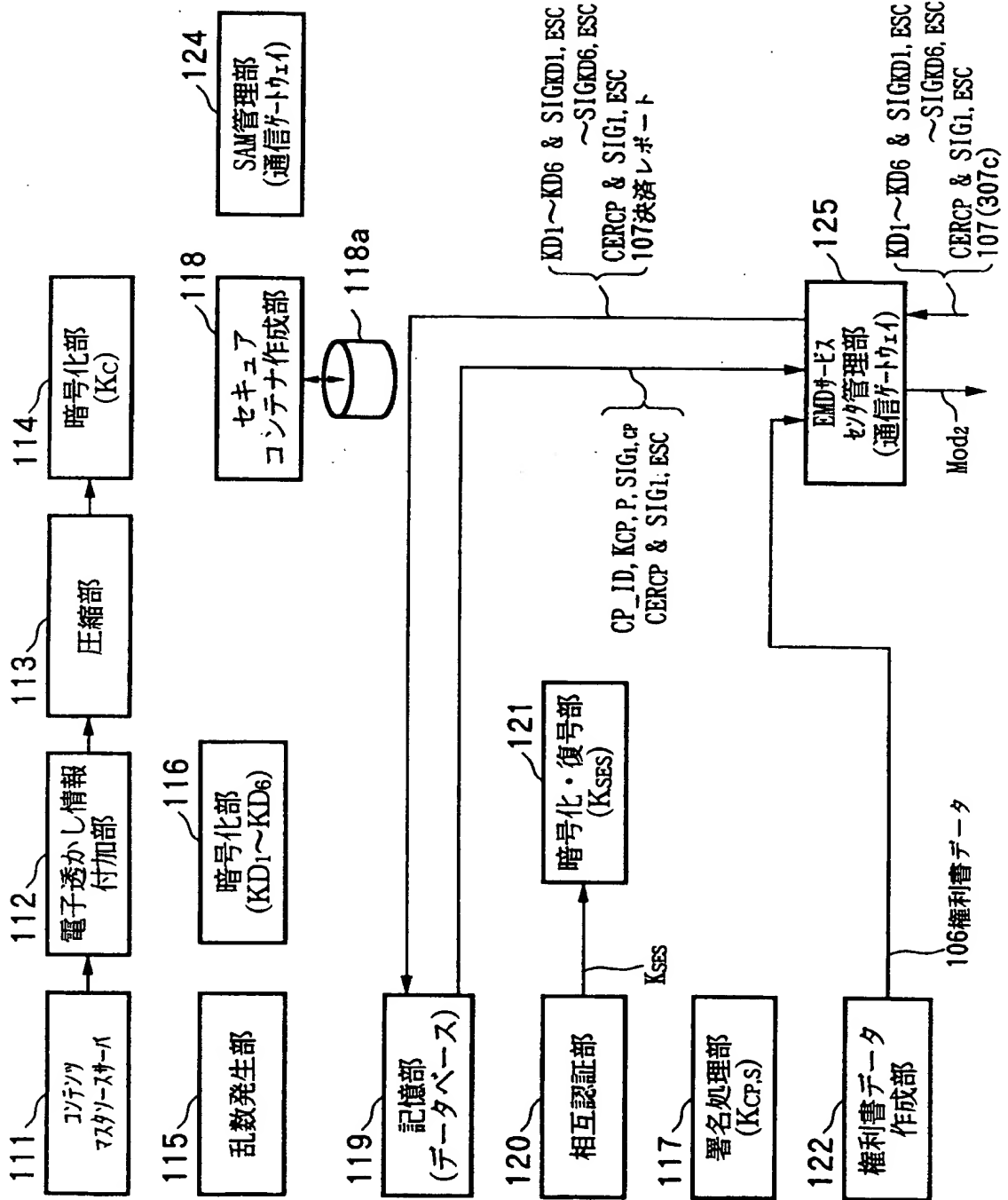
101 コンテンツプロバイダ



THIS PAGE BLANK (USPTO)

FIG.3

101 コンテンツプロバイダ



THIS PAGE BLANK (USPTO)

104 セキュアコンテンツ

FIG.4A

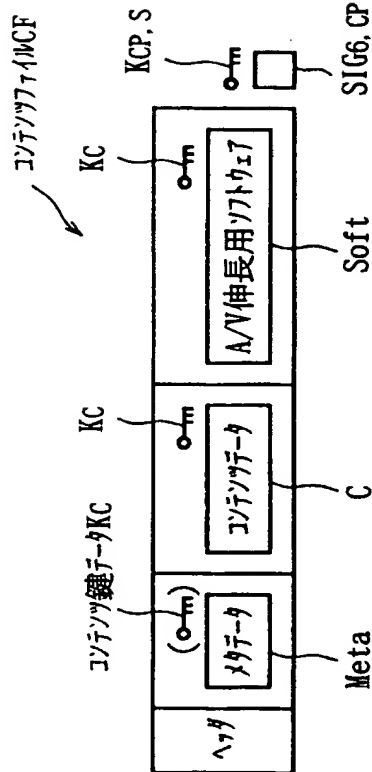


FIG.4B

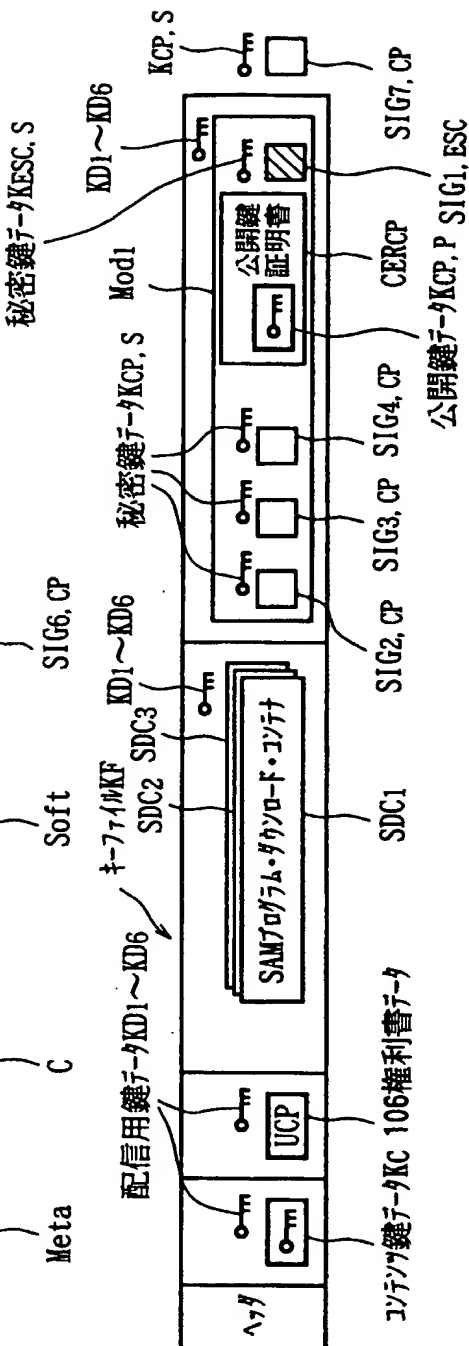
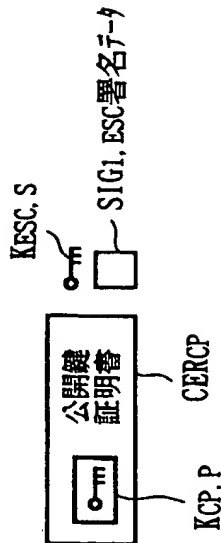


FIG.4C



THIS PAGE BLANK (USPTO)

FIG.5

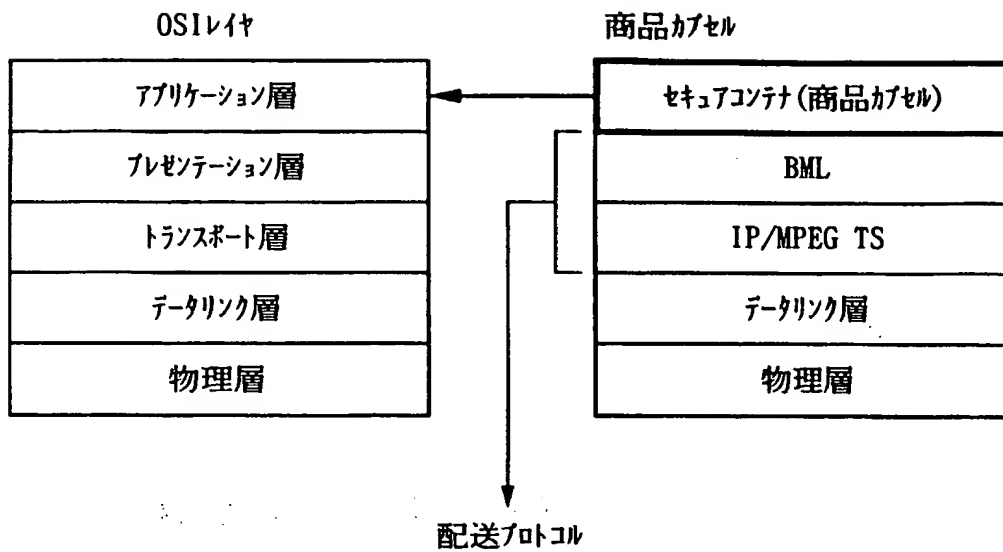
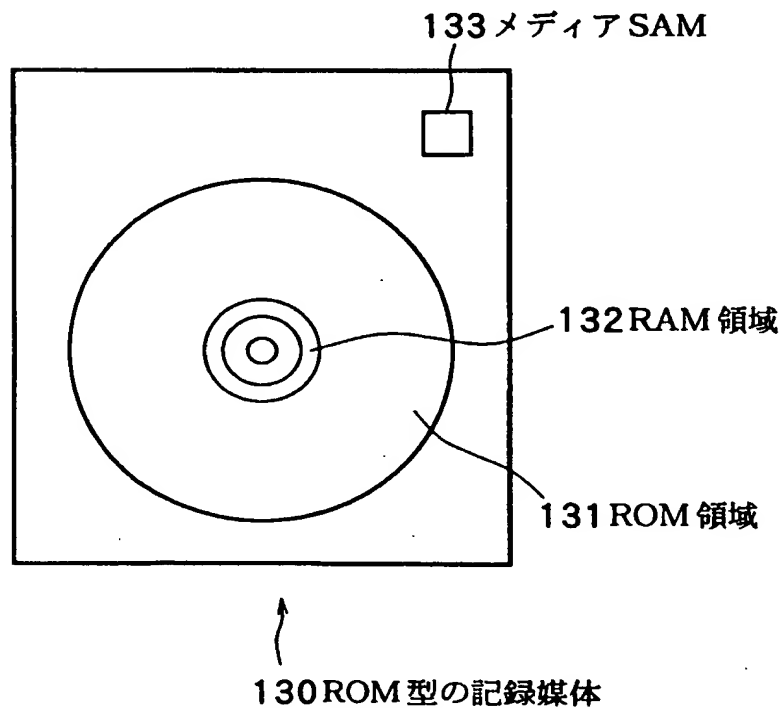
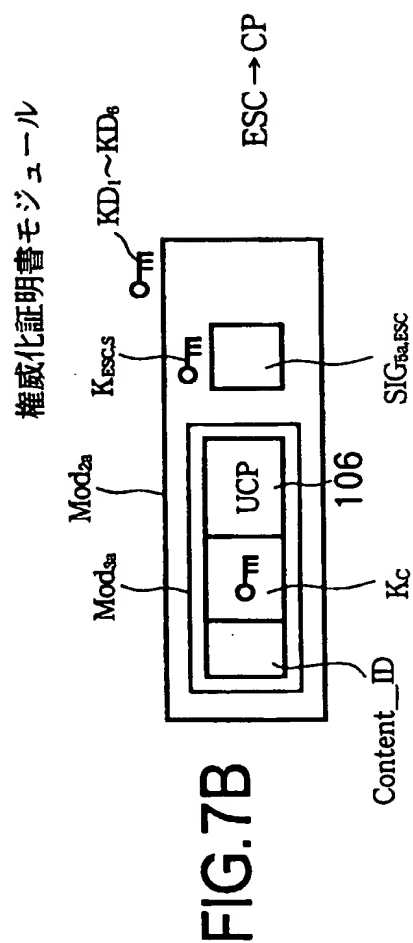
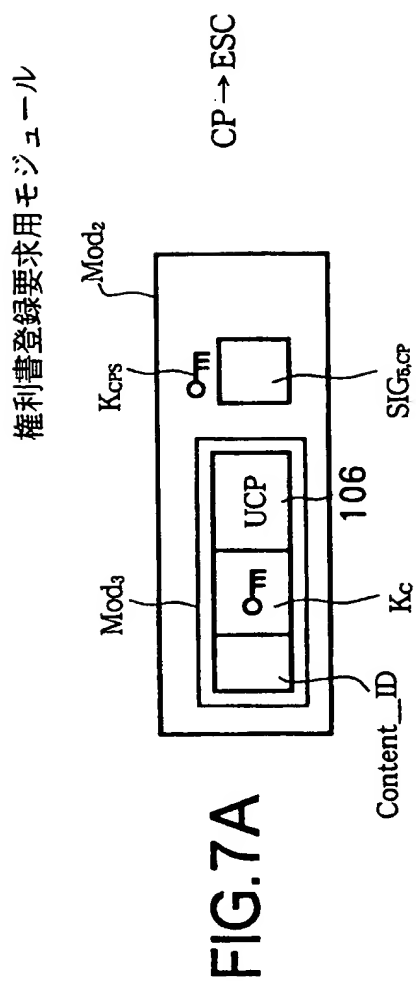


FIG.6

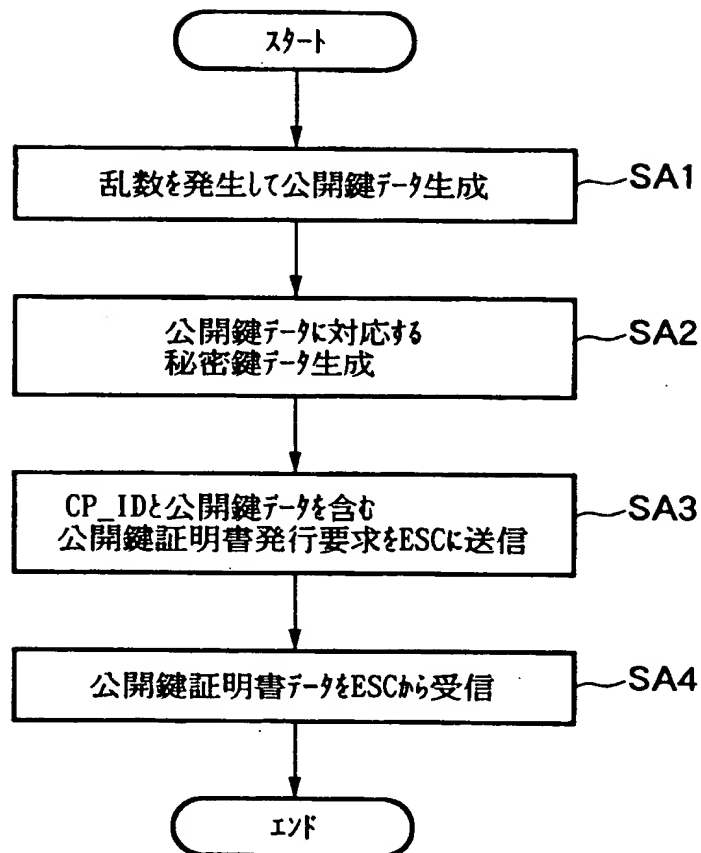


THIS PAGE BLANK (USPTO)



THIS PAGE BLANK (USPTO)

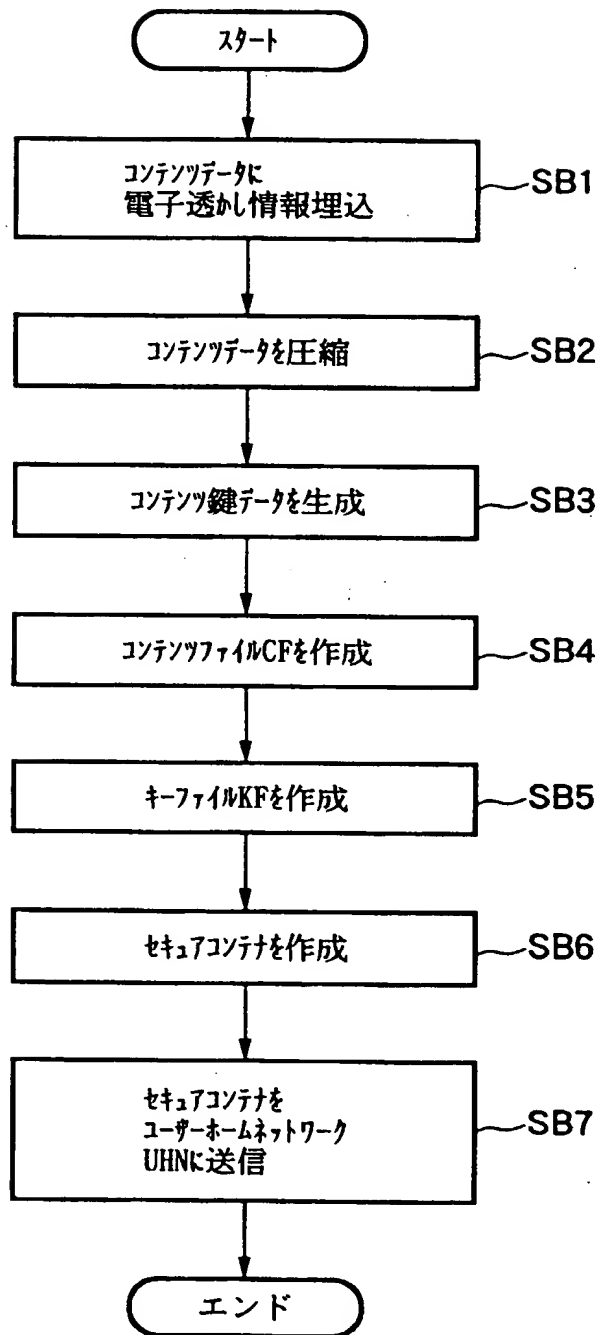
FIG.8



CPからESCへの公開鍵証明書データの発行要求処理

THIS PAGE BLANK (USPTO)

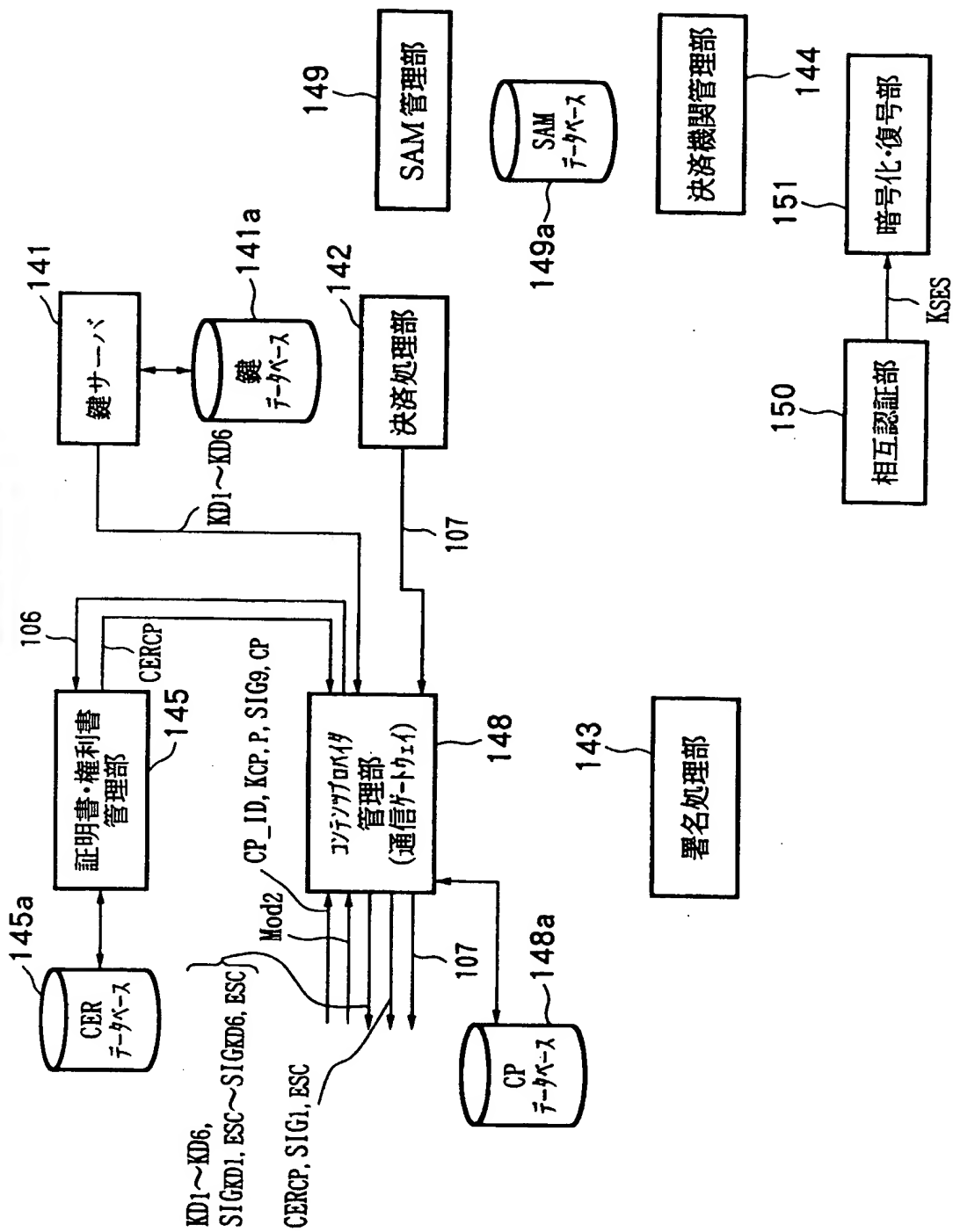
FIG.9

CPのセキュアコンテナ作成処理

THIS PAGE BLANK (USPTO)

FIG.10

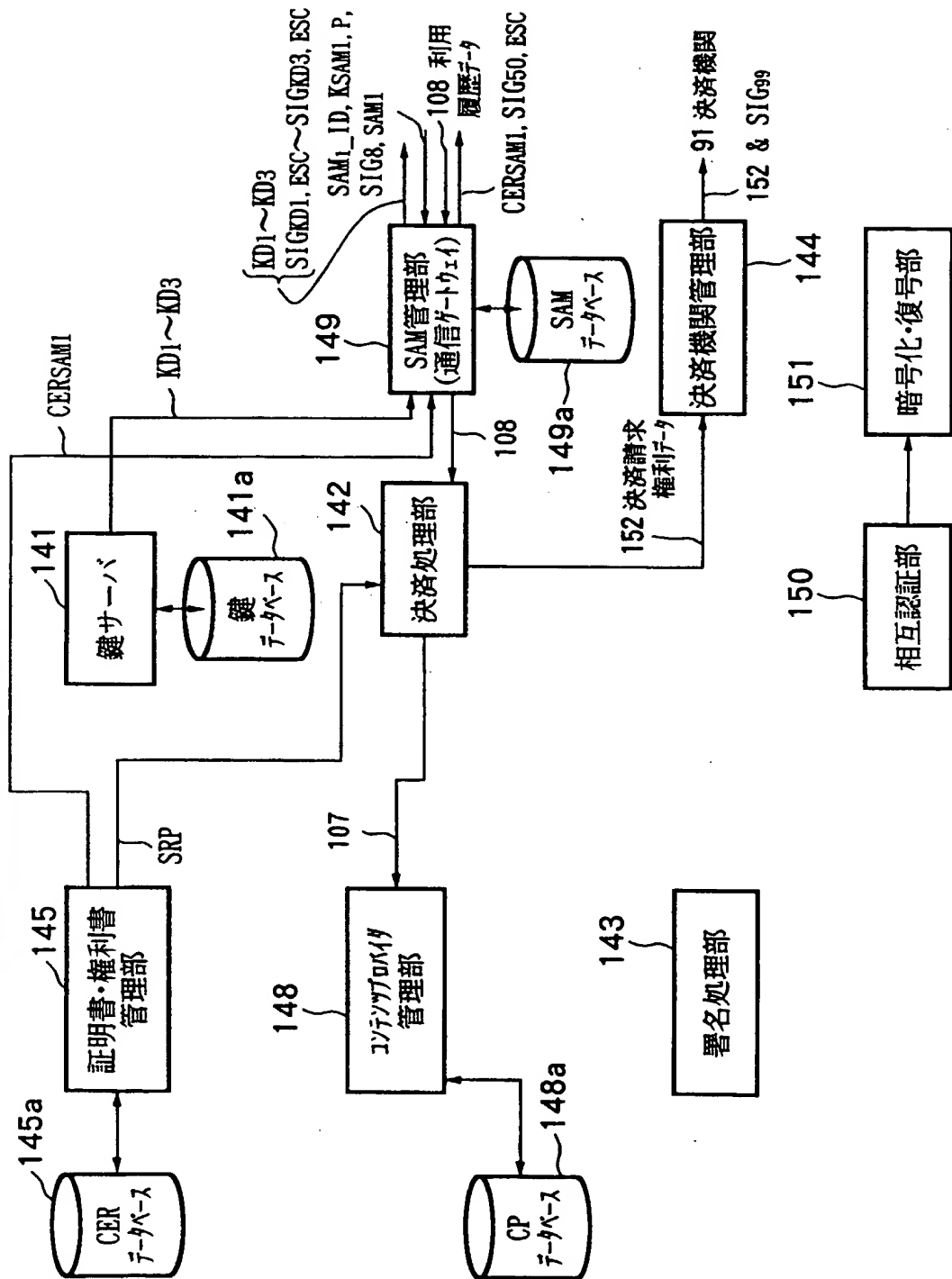
102EMD サービスセンタ



THIS PAGE BLANK (USPTO)

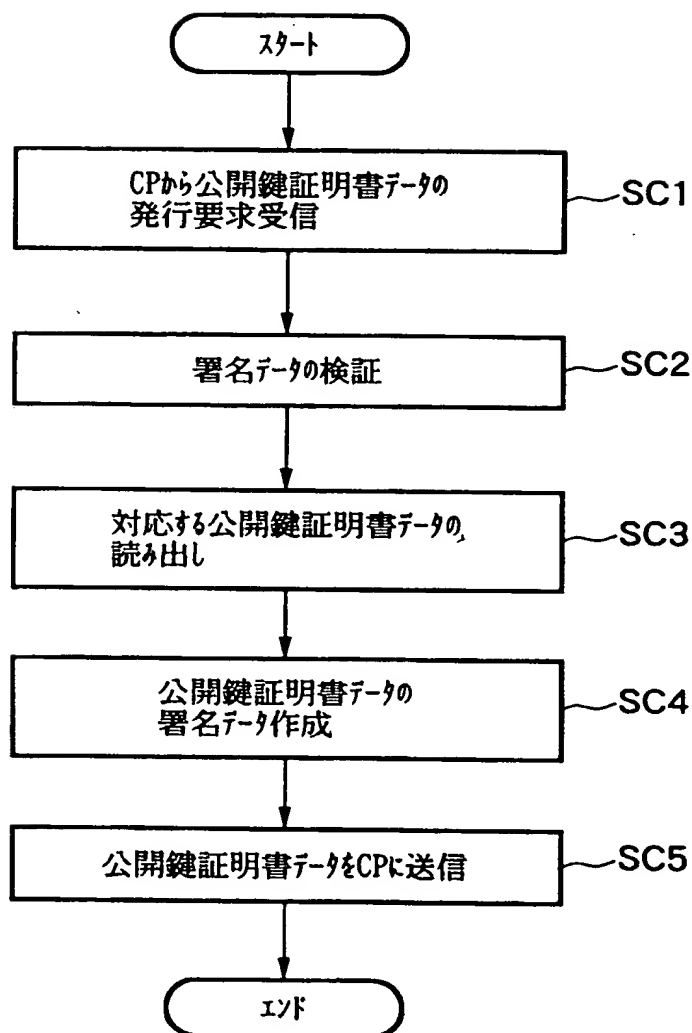
FIG.11

102EMD サービスセンタ



THIS PAGE BLANK (USPTO)

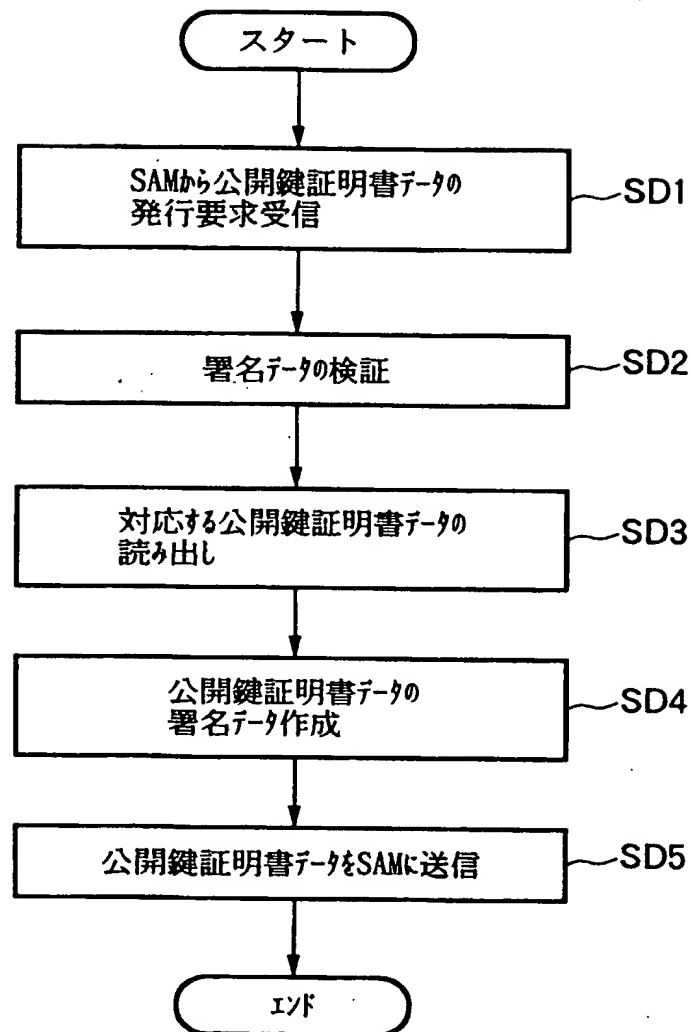
FIG.12



CPからの公開鍵証明書データの発行要求に応じたESCの処理

THIS PAGE BLANK (USPTO)

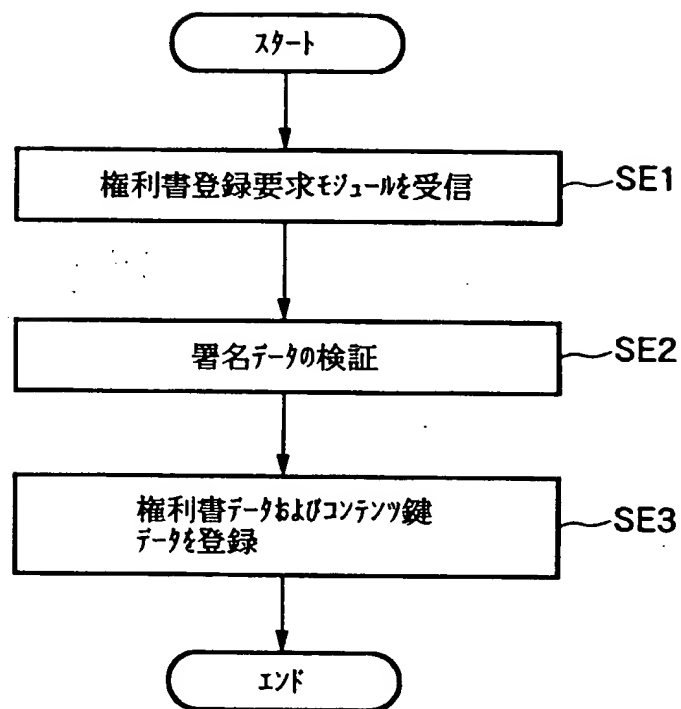
FIG.13



SAMからの公開鍵証明書データの発行要求に応じたESCの処理

THIS PAGE BLANK (08/70)

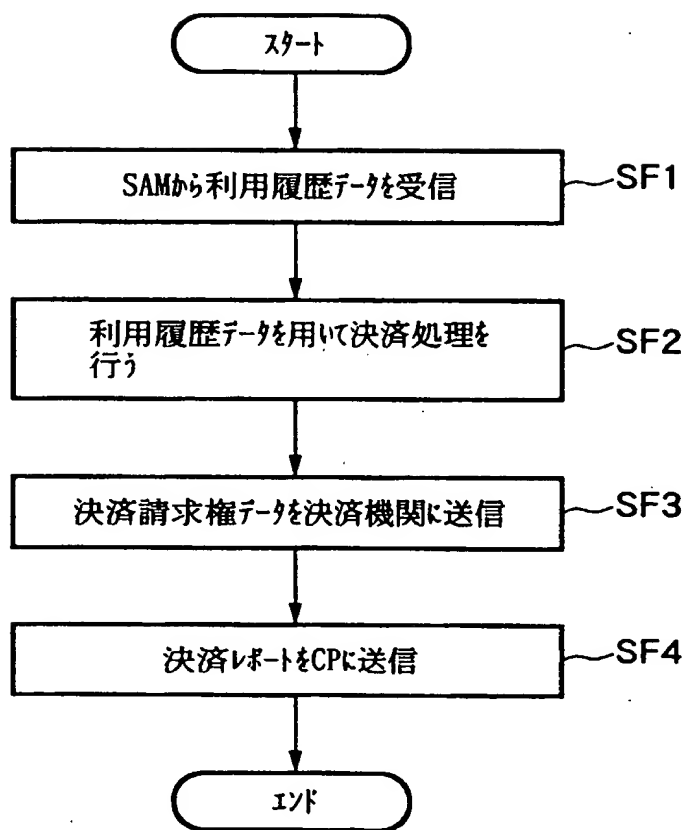
FIG.14



ESCにおける権利書データおよびコンテンツ鍵データの登録処理

THIS PAGE BLANK (USPTO)

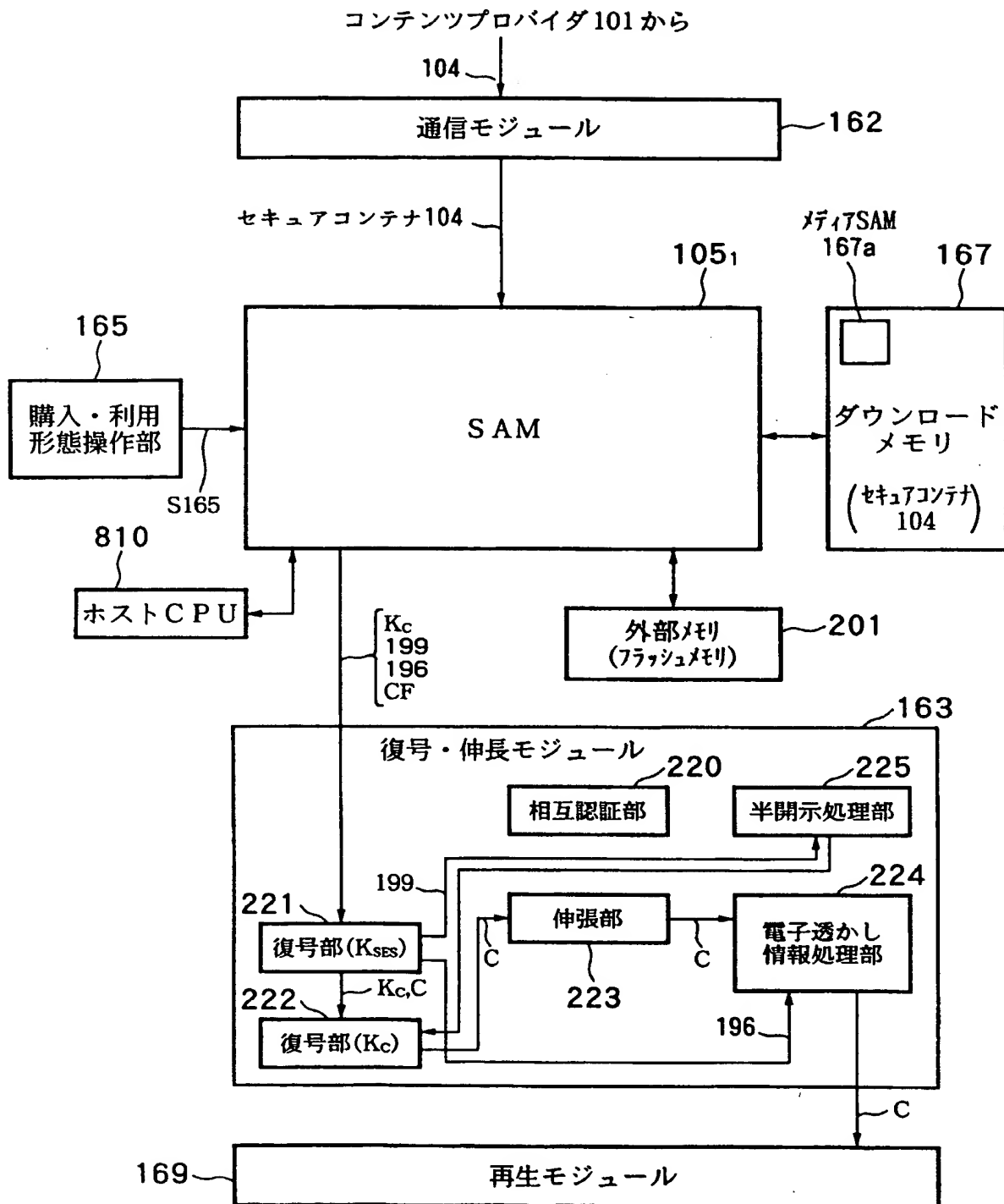
FIG.15



ESCにおける決済処理

THIS PAGE BLANK (USPTO)

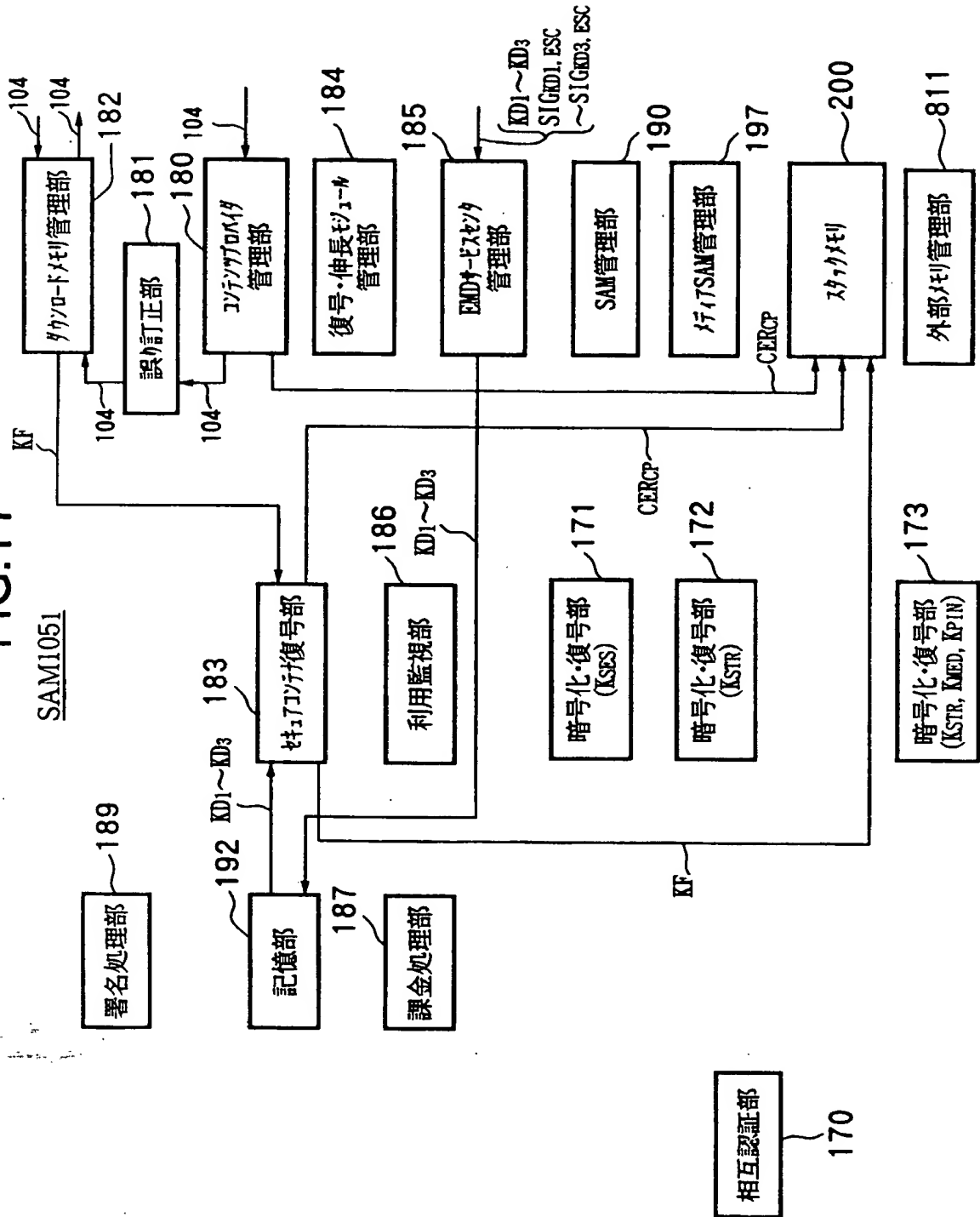
FIG.16



THIS PAGE BLANK (USPTO)

FIG.17

SAM1051



THIS PAGE BLANK (USPTO)

FIG.18

外部メモリ 201 に記憶されるデータ

利用履歴データ 108
SAM 登録リスト

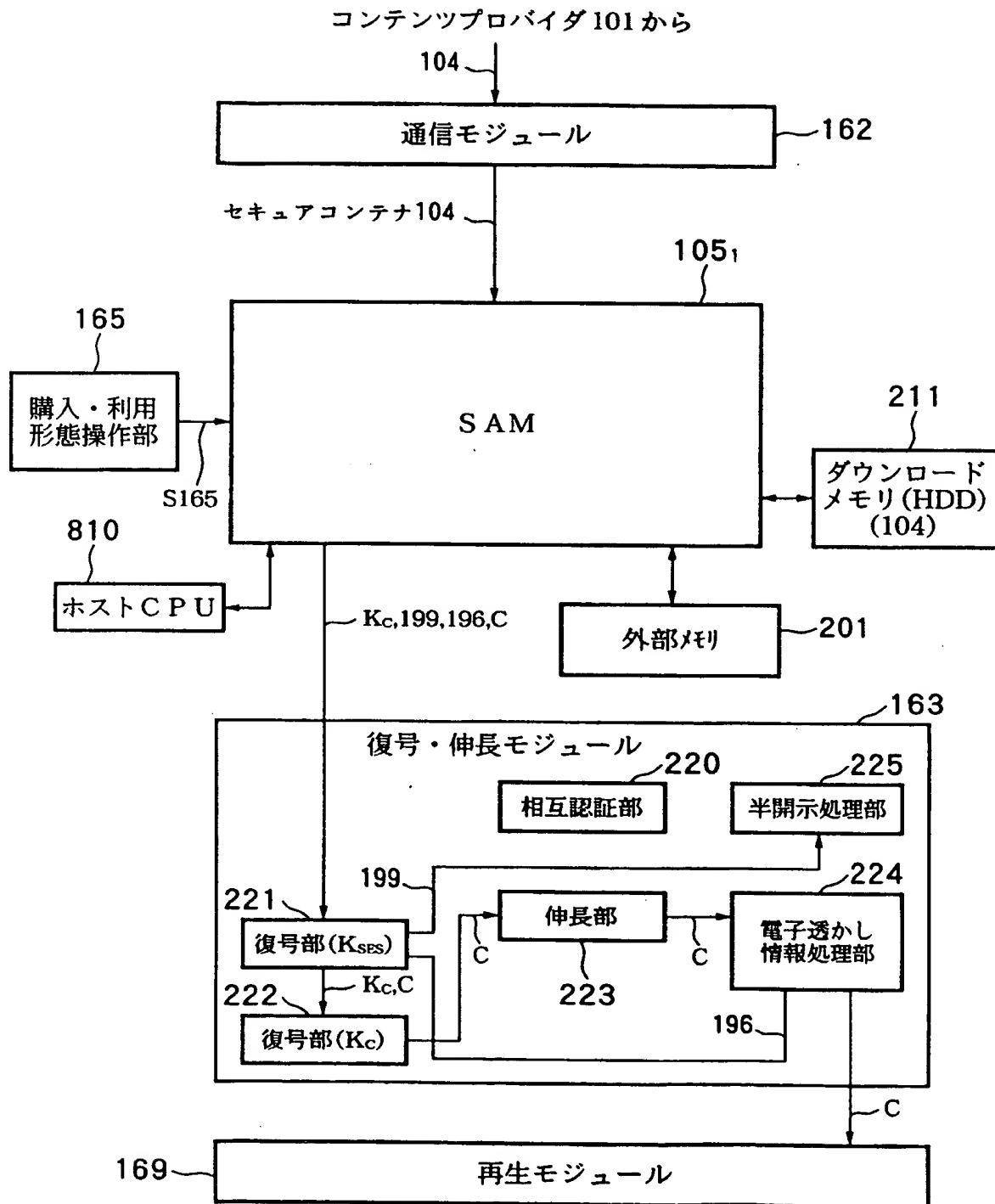
FIG.19

スタックメモリ 200 に記憶されるデータ

コンテンツ鍵データ K_c
権利書データ (UCP) 106
記憶部 (フラッシュメモリ) 192 のロック鍵データ K_{Loc}
コンテンツプロバイダ 101 の公開鍵証明書 CER_{CP}
利用制御情状態データ (UCS) 166
SAM プログラム・ダウンロード・コンテナ $SD_1 \sim SDC_3$

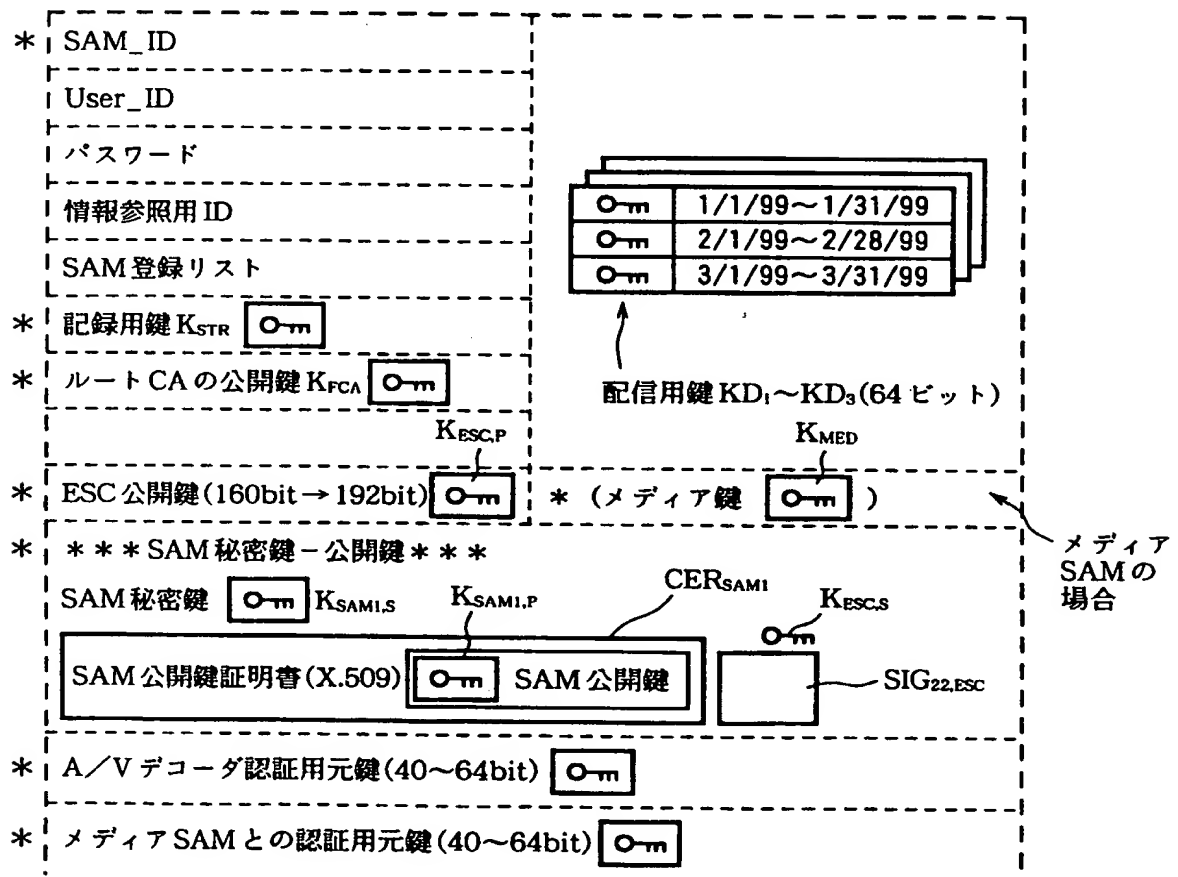
THIS PAGE BLANK (USPTO)

FIG.20



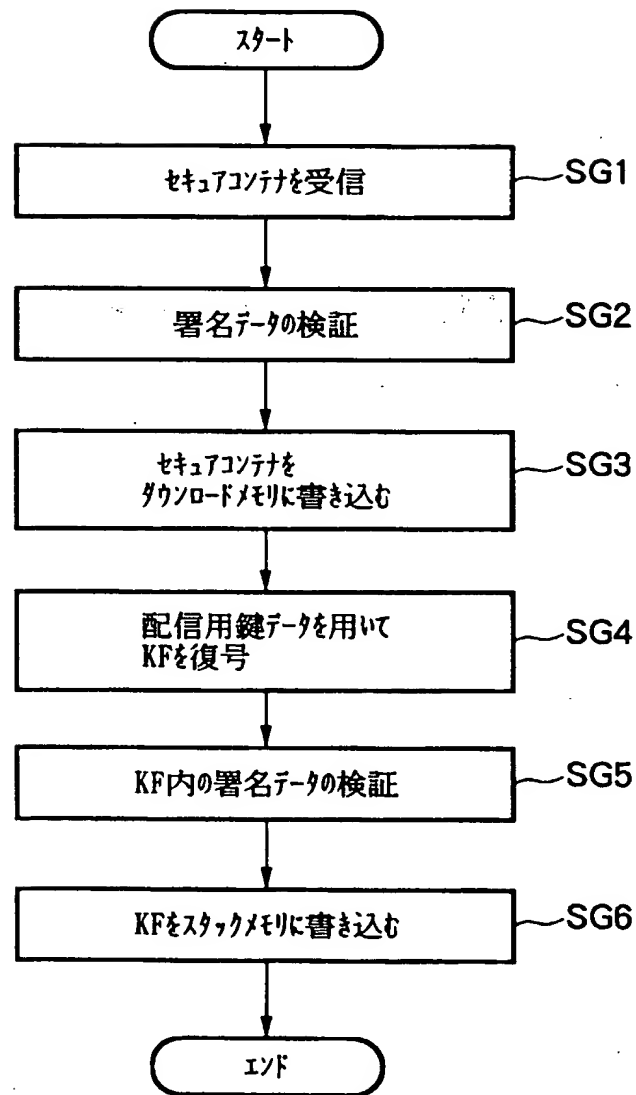
THIS PAGE BLANK (USPTO)

FIG.21

記憶部 192 に記憶されるデータ

THIS PAGE BLANK (USPTO)

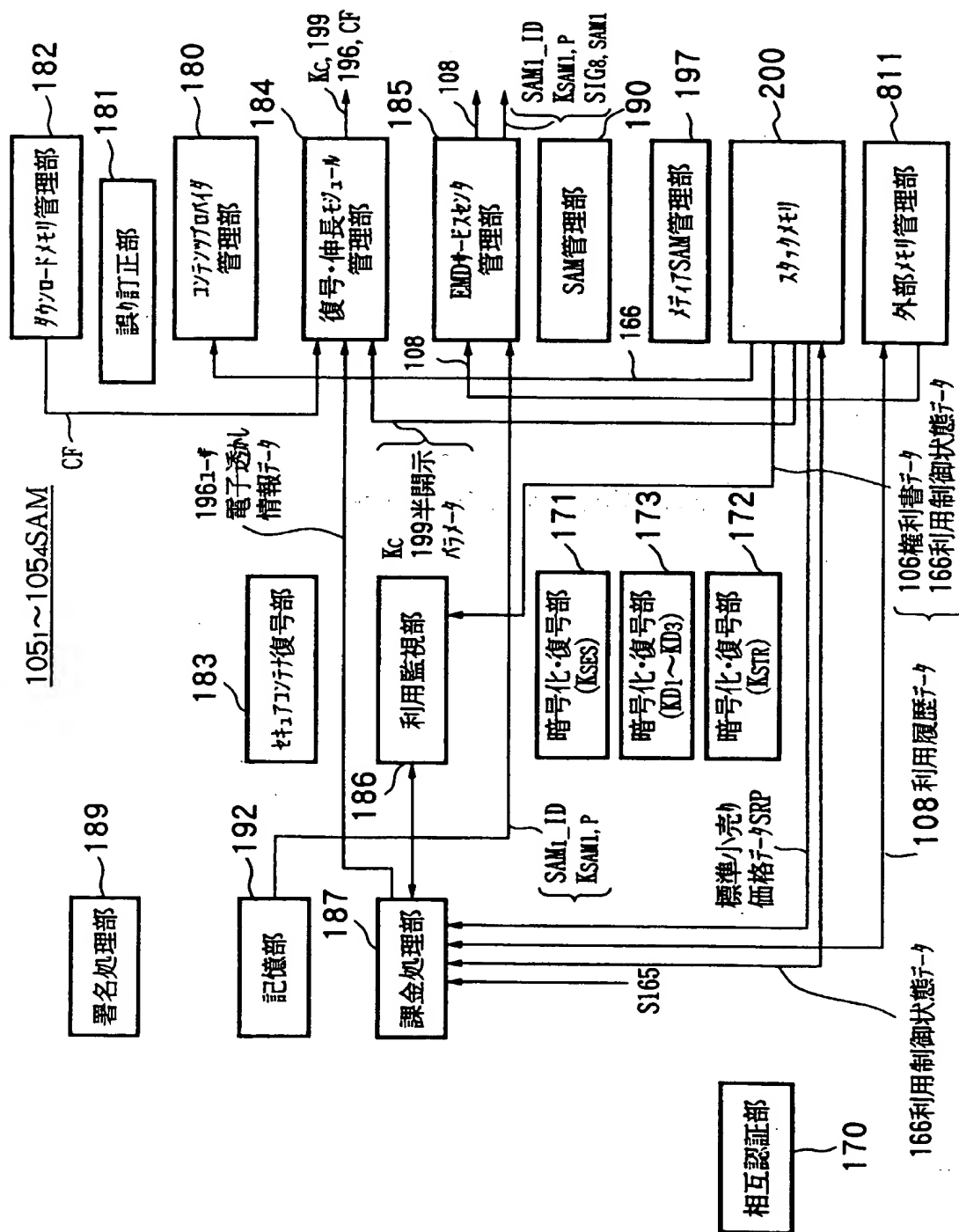
FIG.22



SAMにおけるKFの復号処理

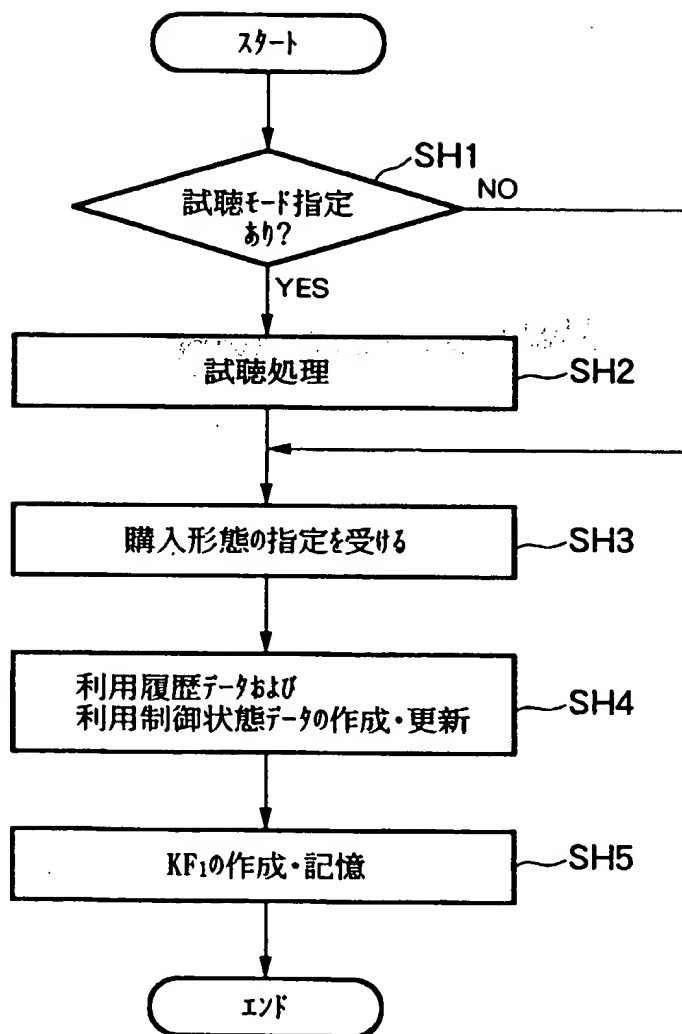
THIS PAGE BLANK (USPTO)

FIG.23



THIS PAGE BLANK (USPTO)

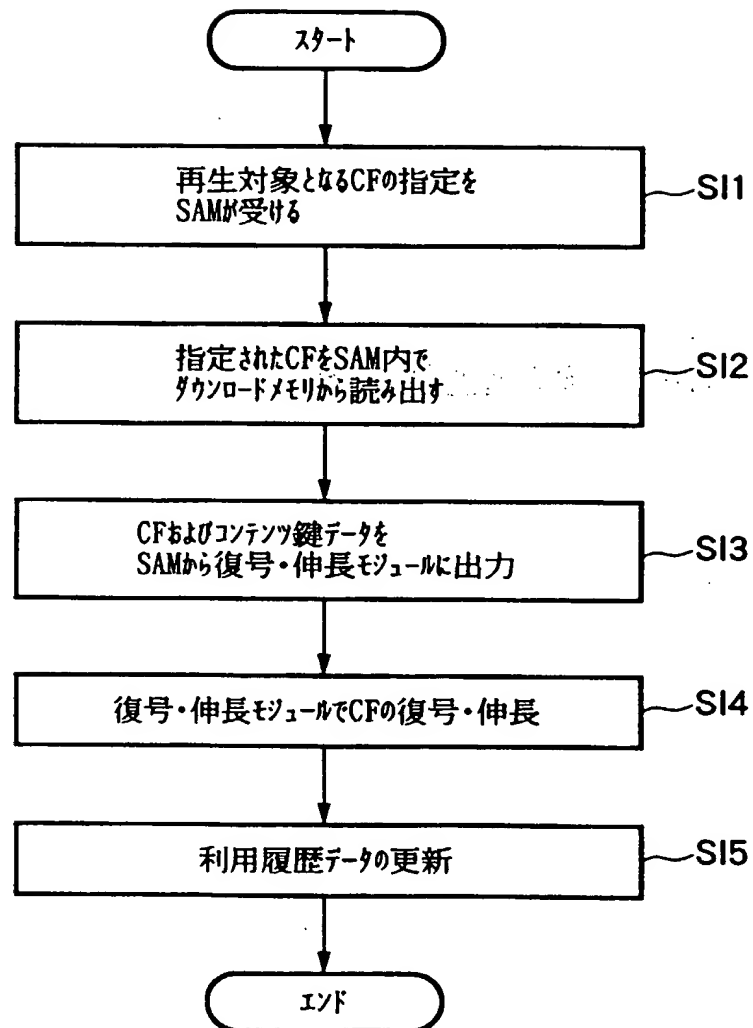
FIG.24



SAMにおけるセキュアコンテナの購入形態決定処理

THIS PAGE BLANK (USPTO)

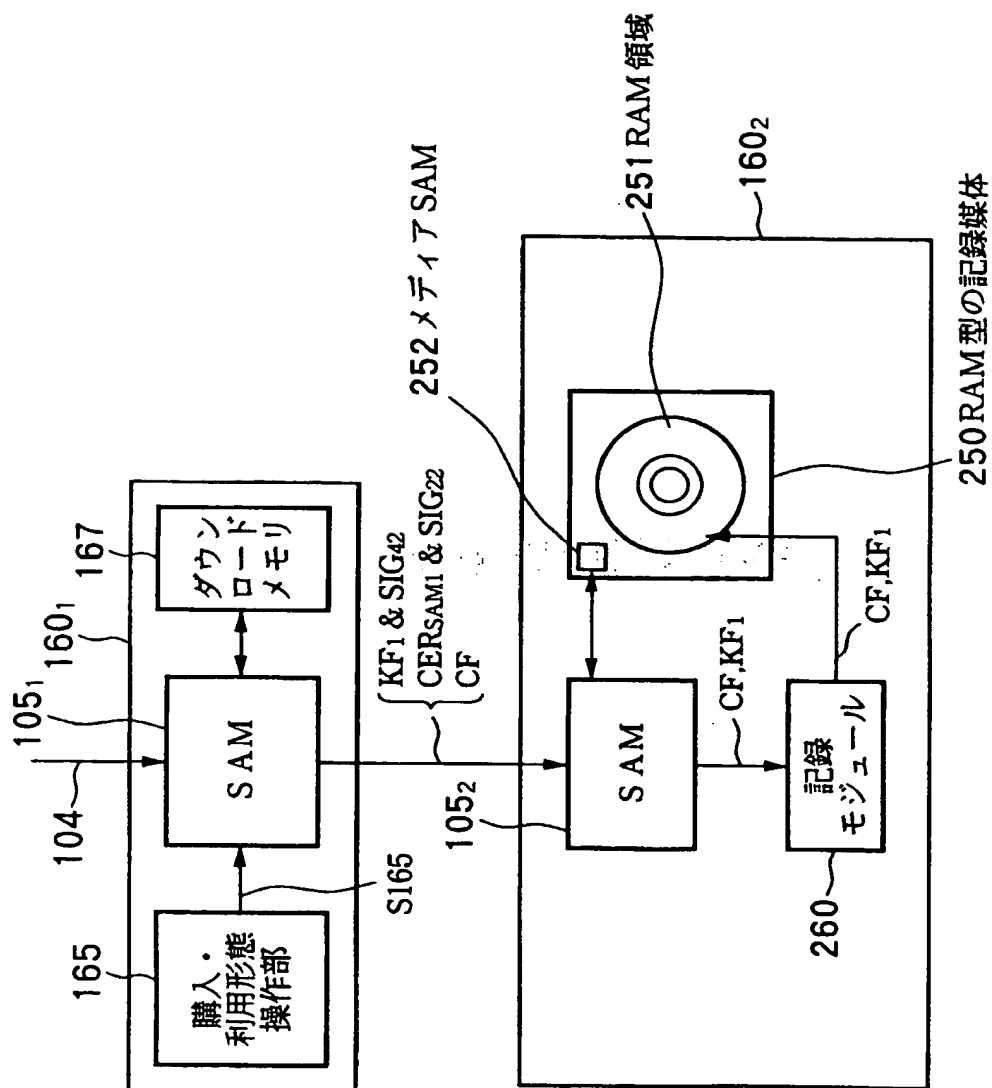
FIG.25



コンテンツデータの再生処理

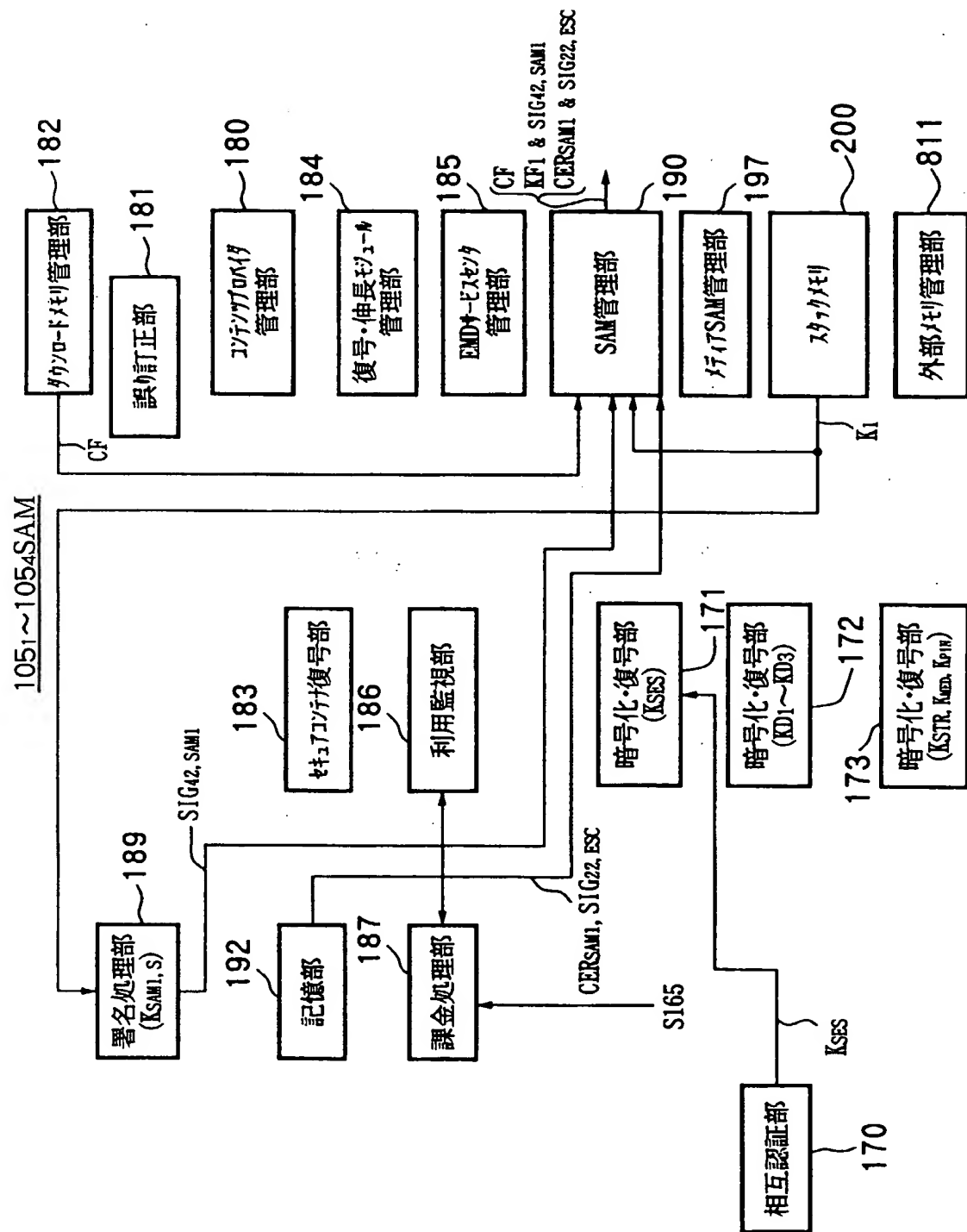
THIS PAGE BLANK (USPTO)

FIG.26



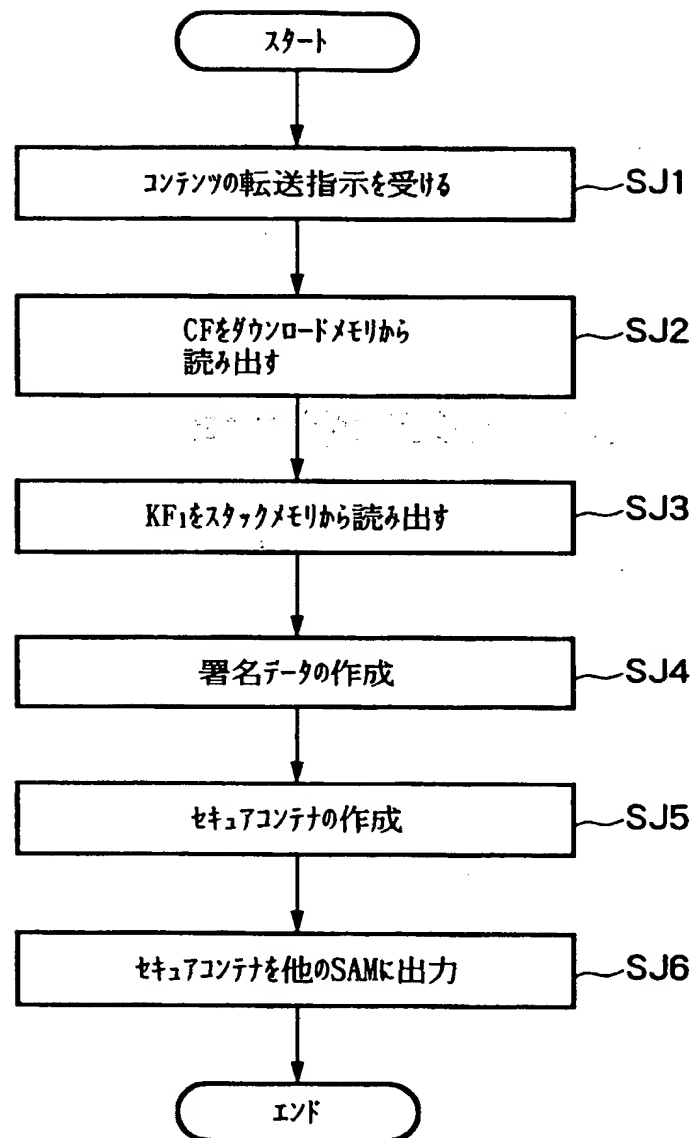
THIS PAGE BLANK (USPTO)

FIG27



THIS PAGE BLANK (USPTO)

FIG.28



購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

THIS PAGE BLANK (USPTO)

購入形態が決定したセキュアコンテンツ

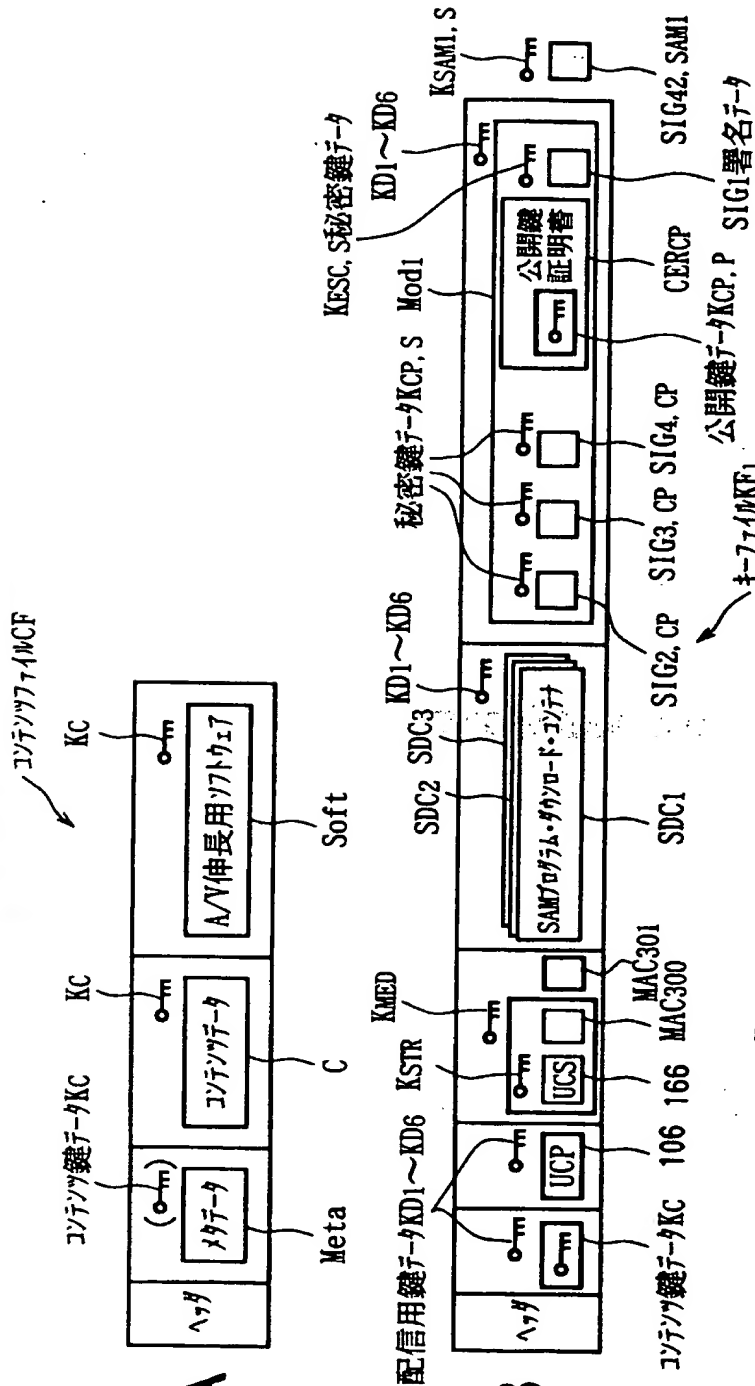


FIG. 29A

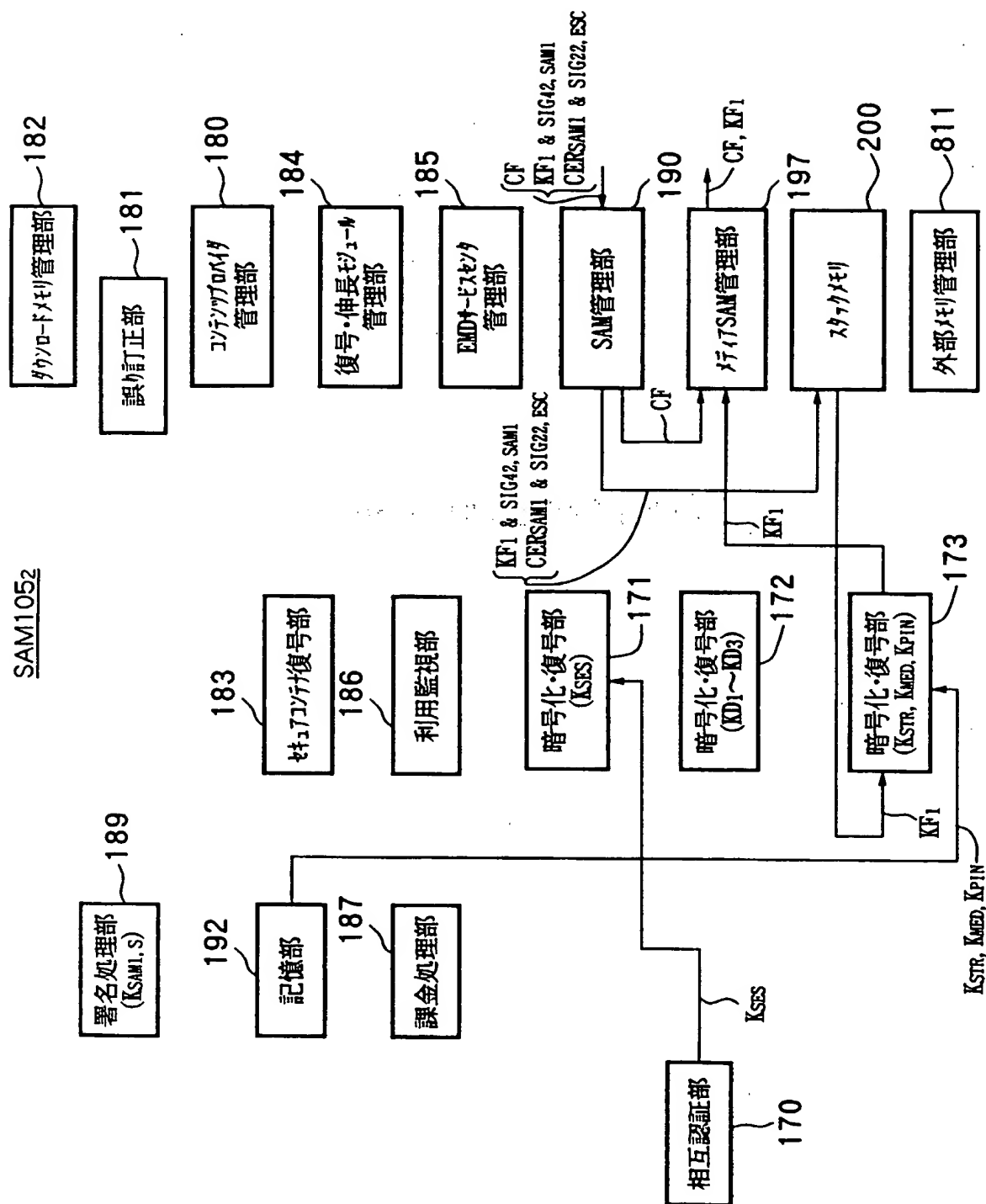
FIG. 29B

FIG. 29C

THIS PAGE BLANK (USPTO)

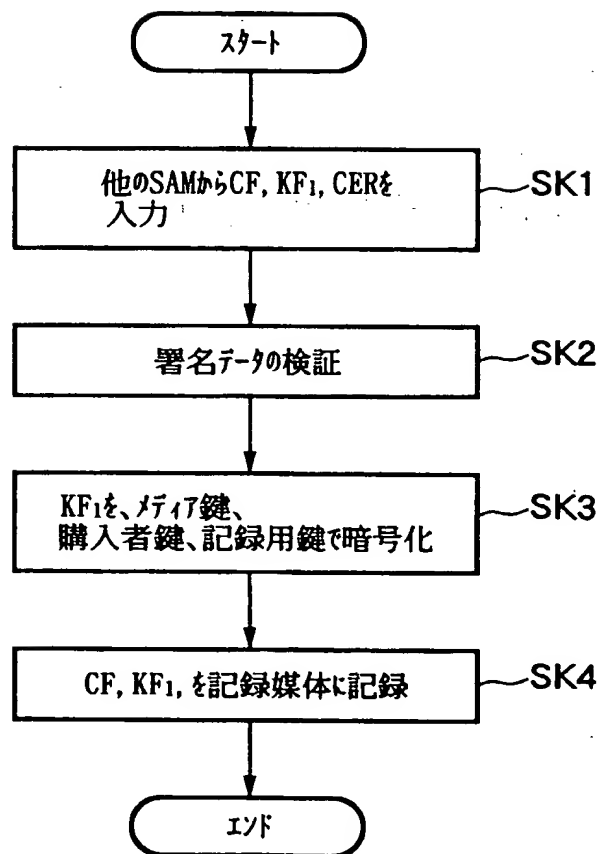
FIG. 30

SAM1052



THIS PAGE BLANK (USPTO)

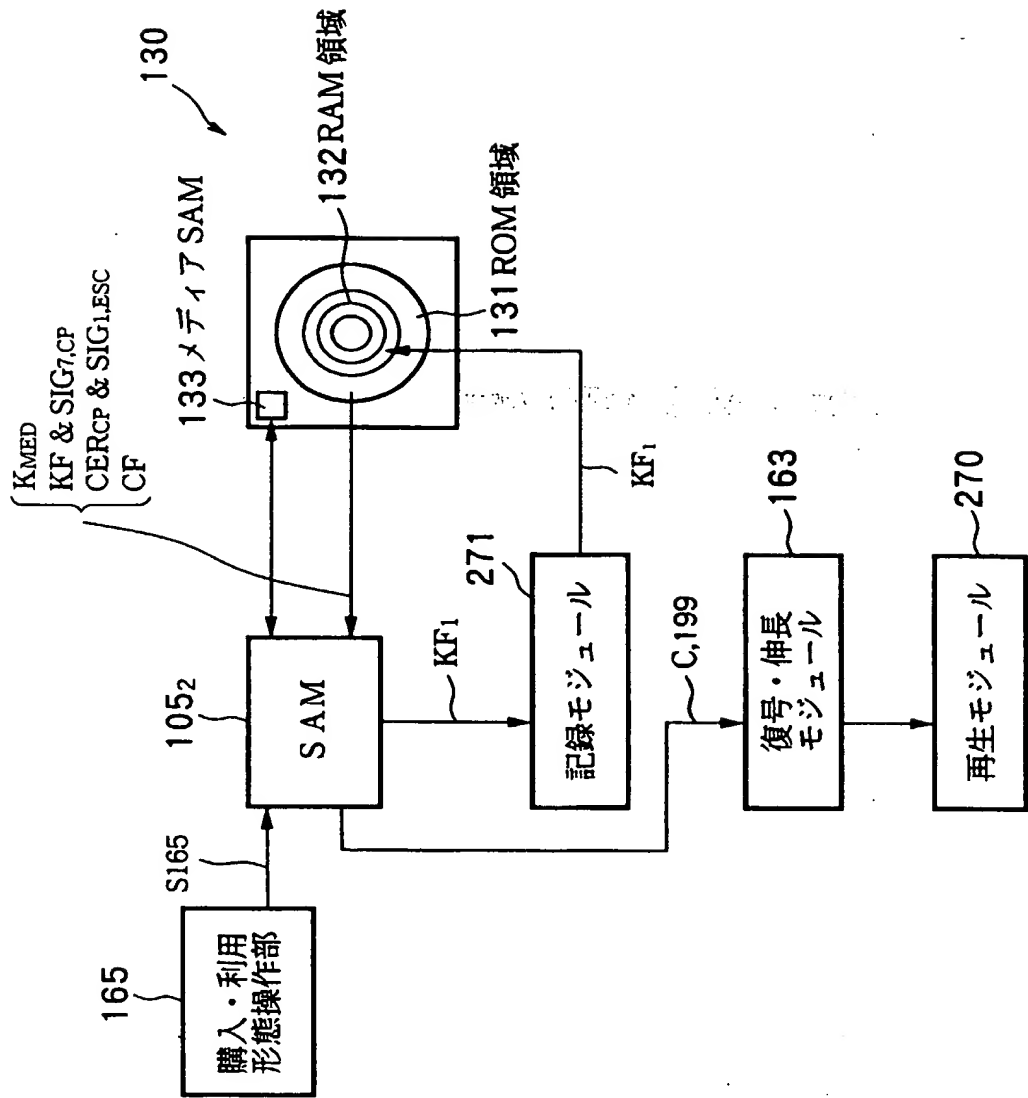
FIG.31



他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

THIS PAGE BLANK (USPTO)

FIG.32

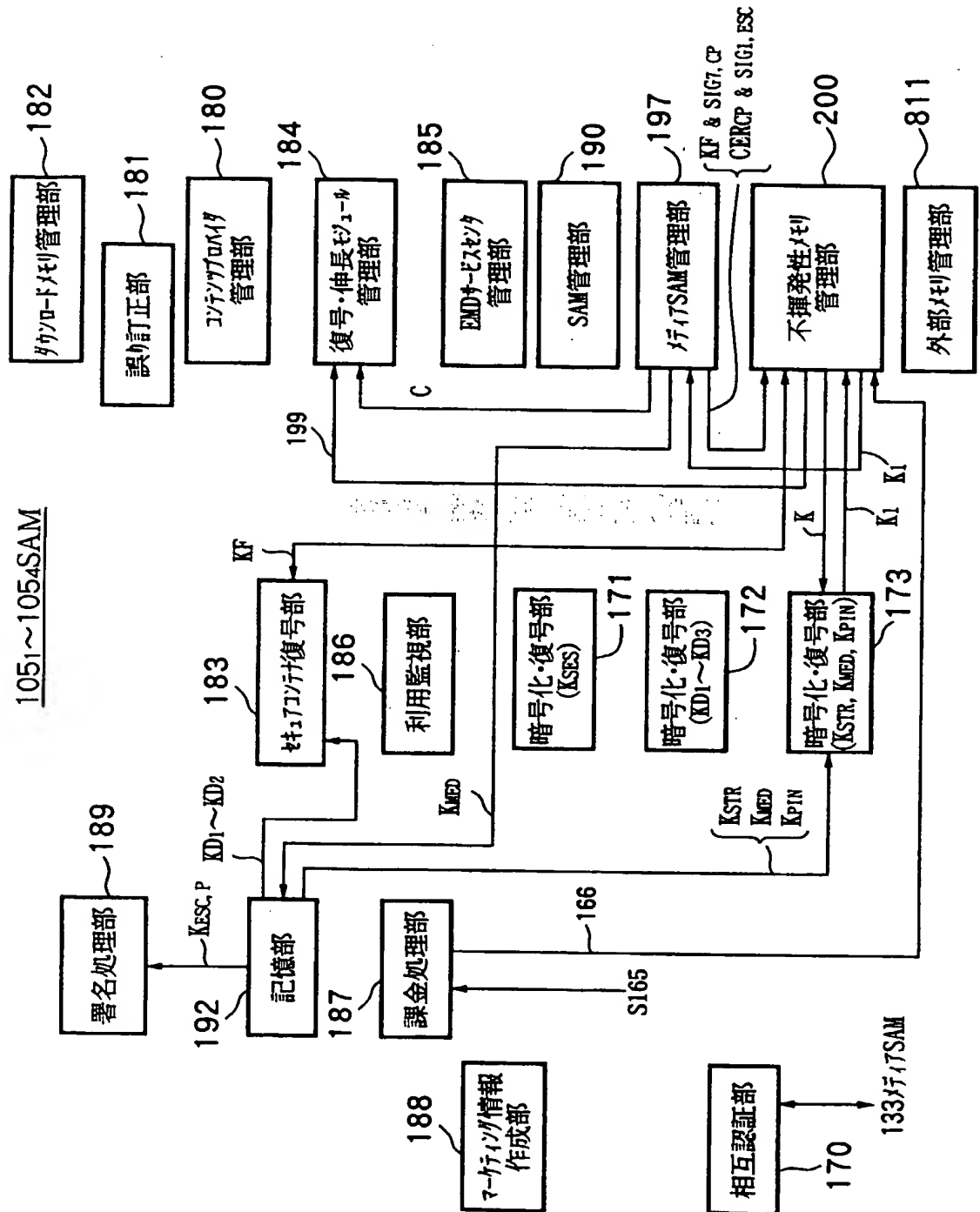


160₂

THIS PAGE BLANK (USPTO)

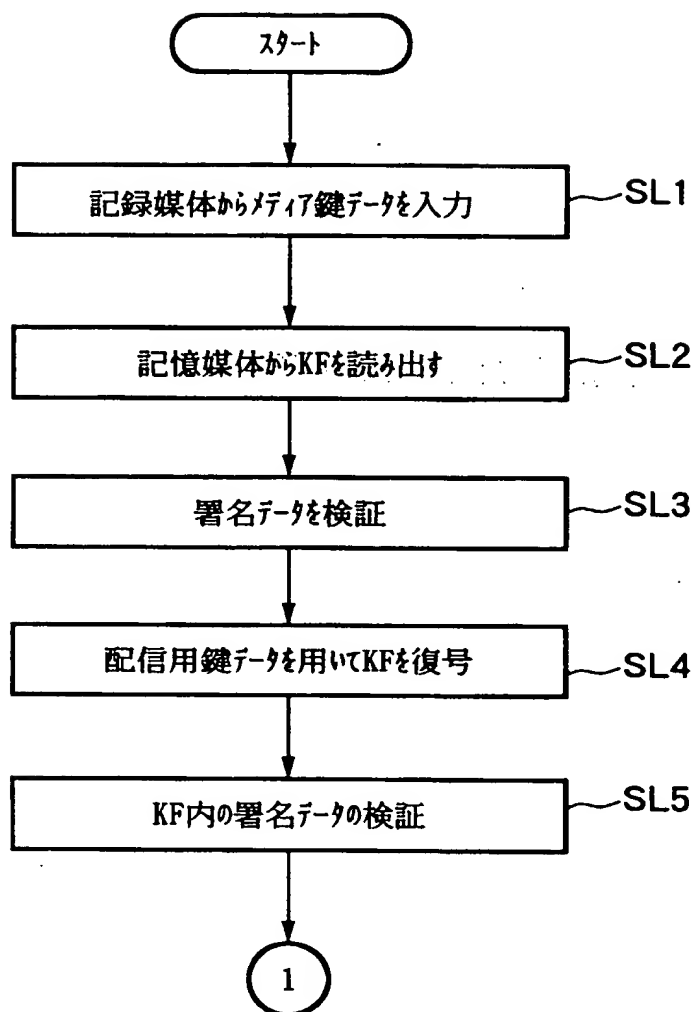
FIG.33

1051~1054SAM



THIS PAGE BLANK (USPTO)

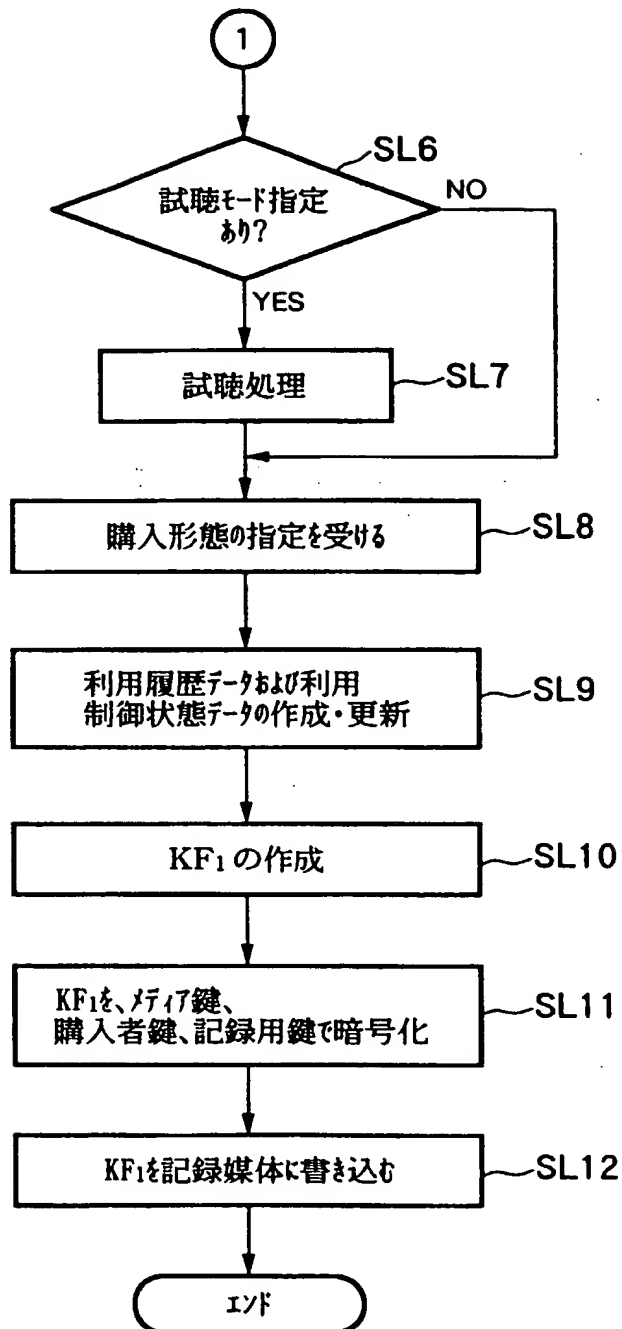
FIG.34



オンラインで配給されたコンテンツのSAMにおける購入形態決定処理

THIS PAGE BLANK (USPTO)

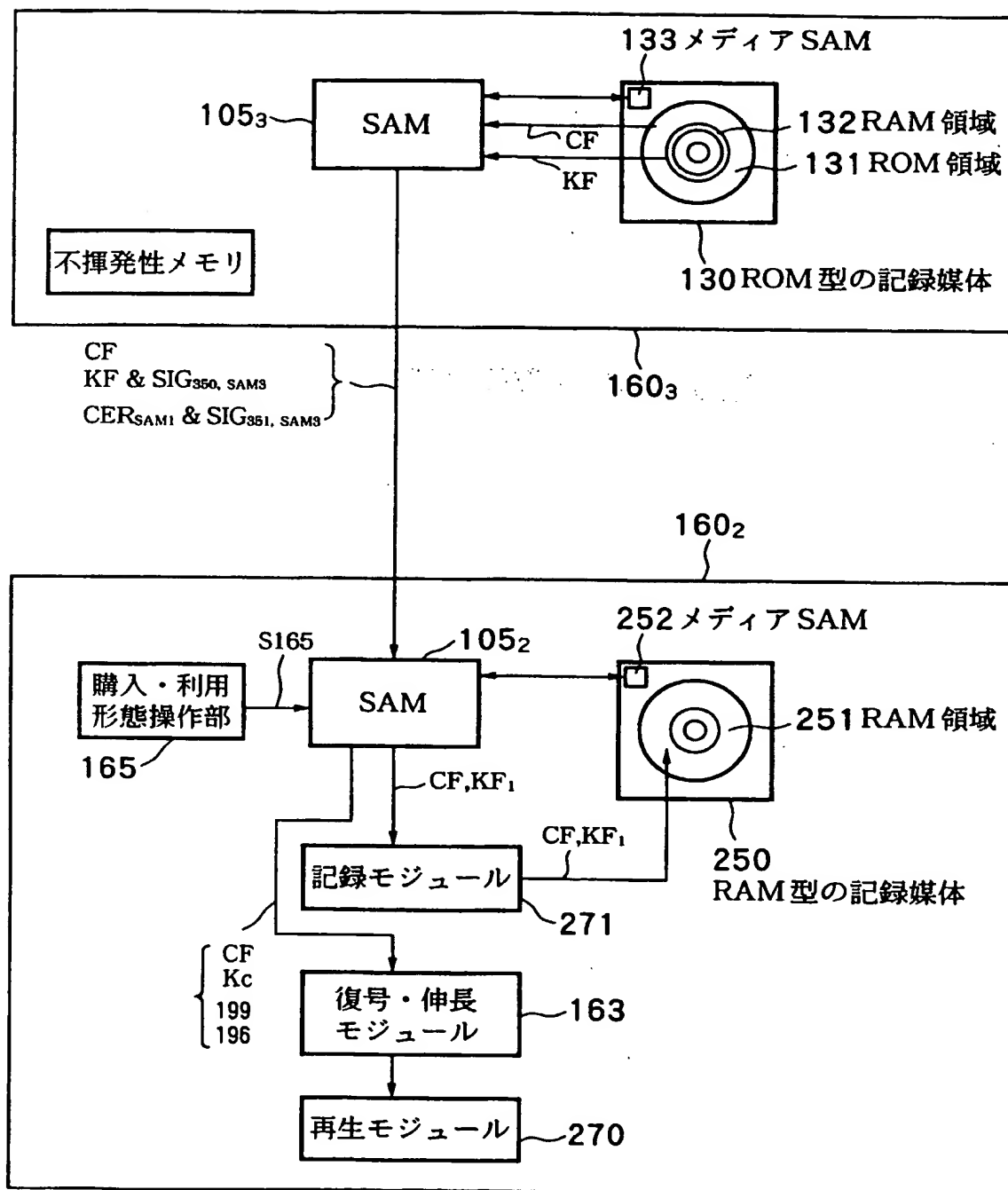
FIG.35



オフラインで配給されたコンテンツのSAMにおける購入形態決定処理

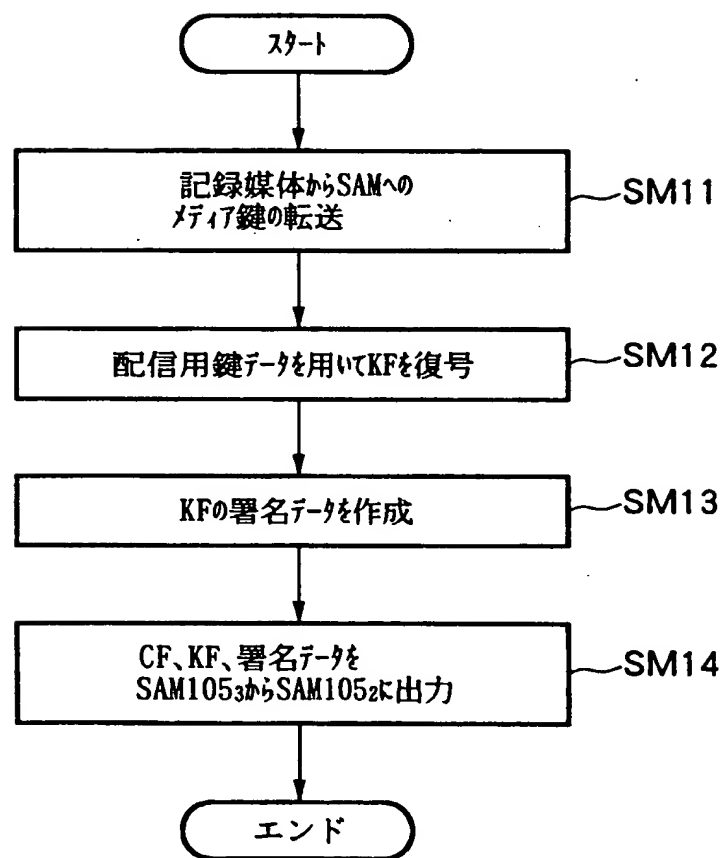
THIS PAGE BLANK (USPTO)

FIG.36



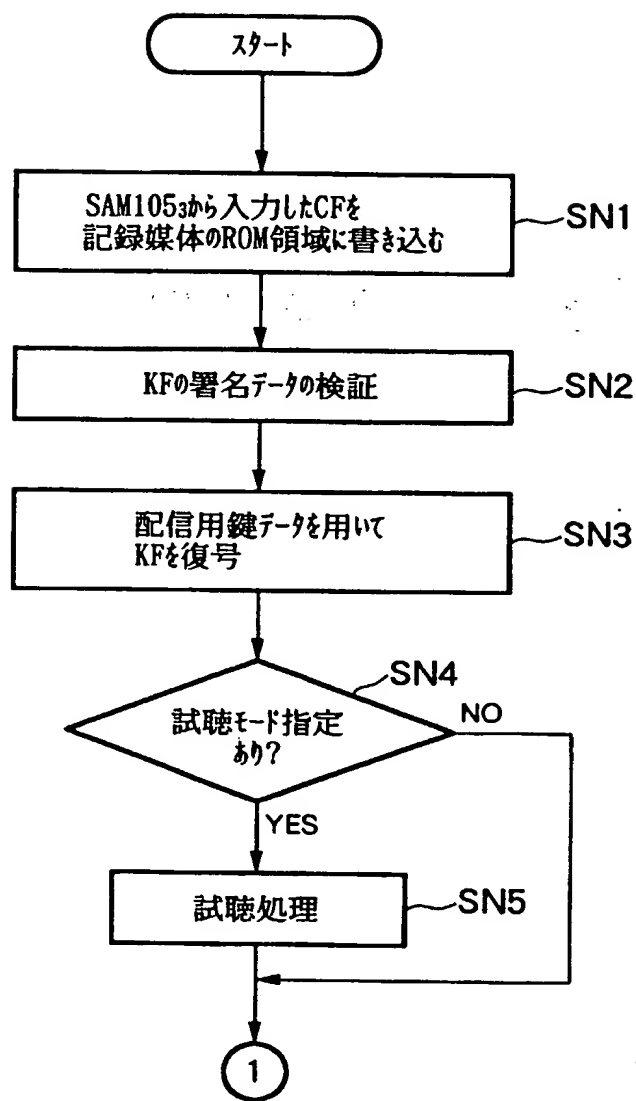
THIS PAGE BLANK (USPTO)

FIG.37

SAM1053の処理

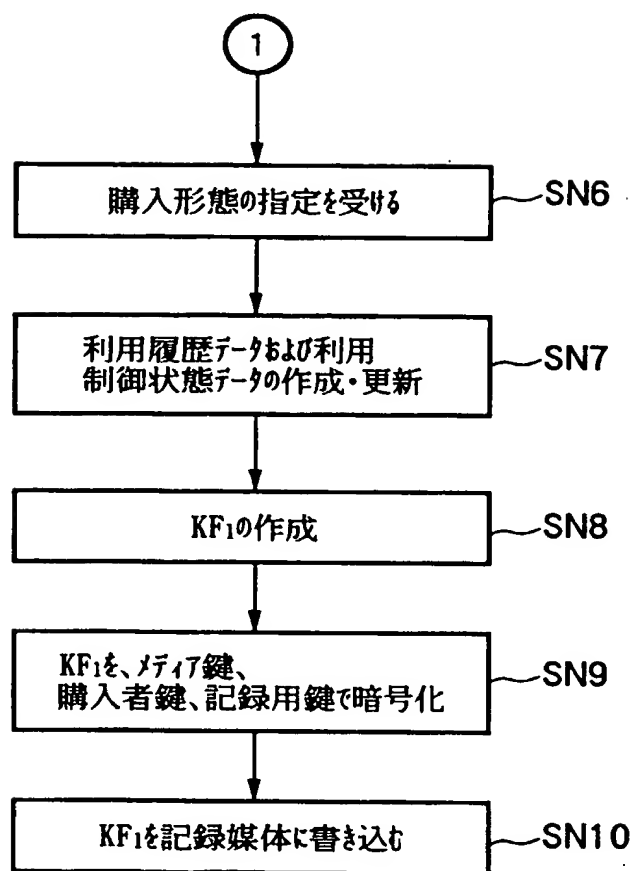
THIS PAGE BLANK (USPTO)

FIG.38

SAM1052の処理

THIS PAGE BLANK (USPTO)

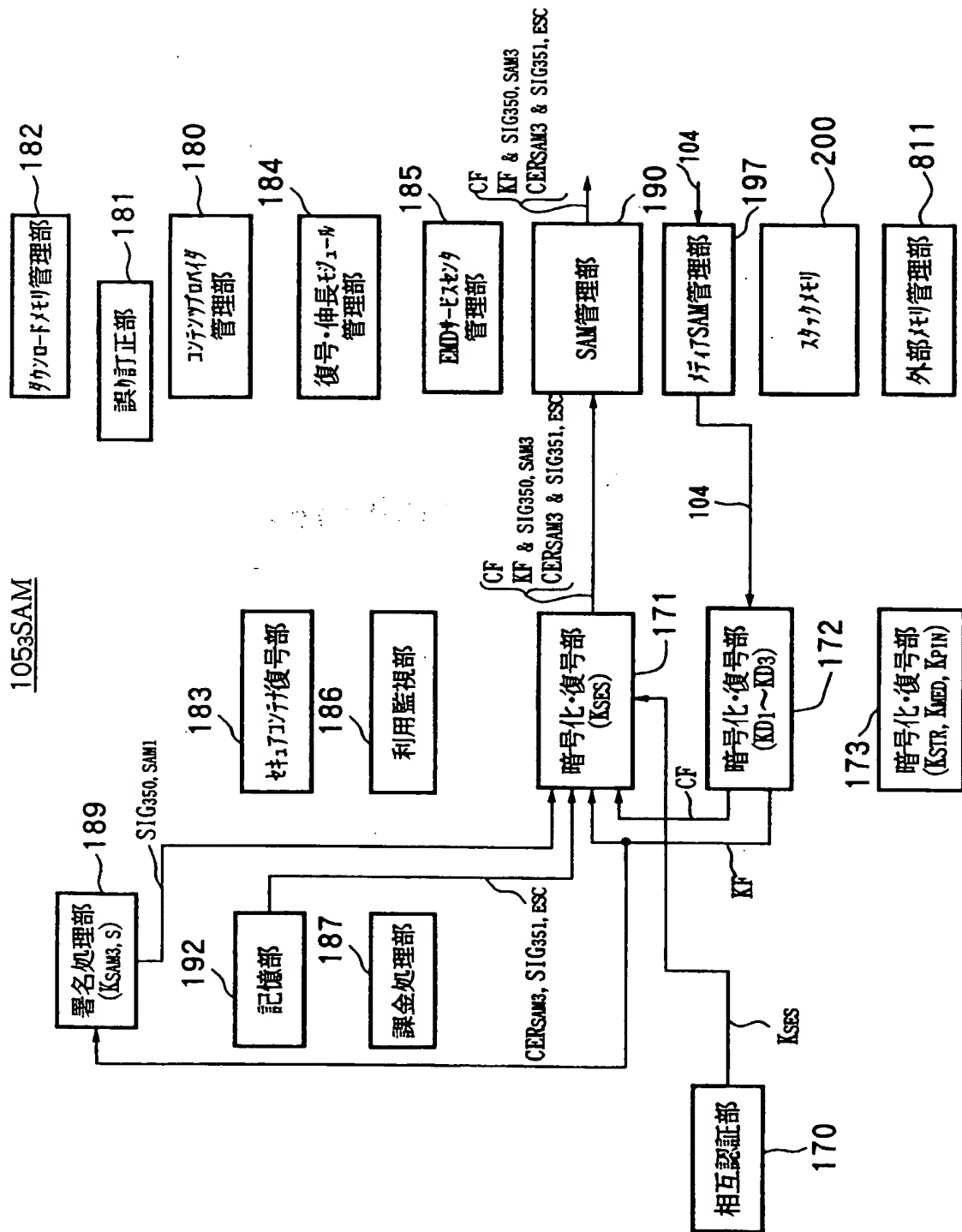
FIG.39

SAM105₂の処理

THIS PAGE BLANK (USPTO)

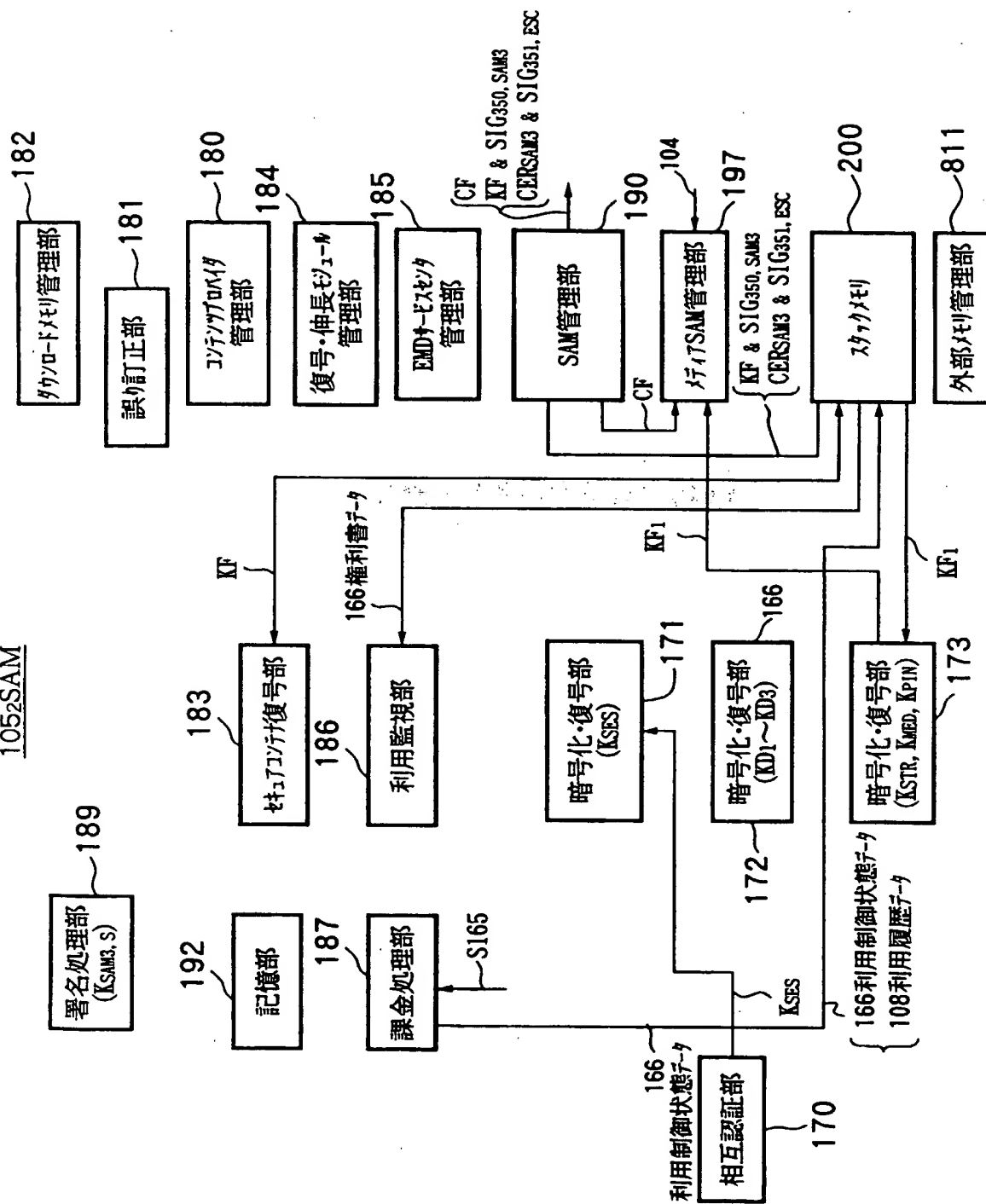
FIG. 40

1053SAM



THIS PAGE BLANK (USPTO)

FIG. 41

1052SAM

THIS PAGE BLANK (USPTO)

FIG.42A 101 (CP) → SAM105₁
(イン・バンド)

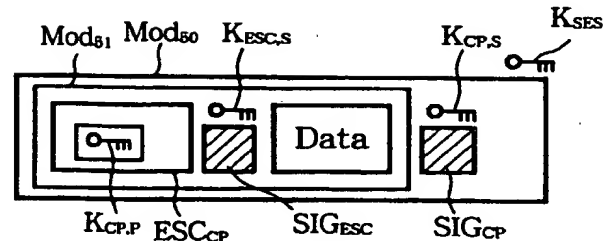


FIG.42B 101 (CP) → SAM105₁
(アウト・オブ・バンド)

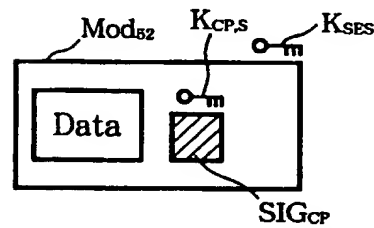


FIG.42C 102 (ESC) → SAM105₁
(アウト・オブ・バンド)

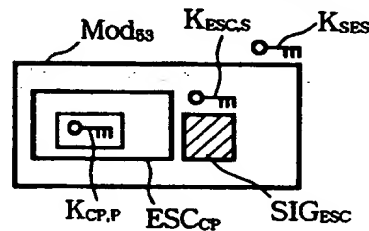


FIG.42D SAM105₁ → 101 (CP)
(イン・バンド)

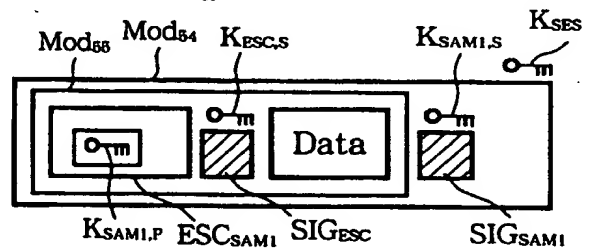


FIG.42E SAM105₁ → 101 (CP)
(アウト・オブ・バンド)

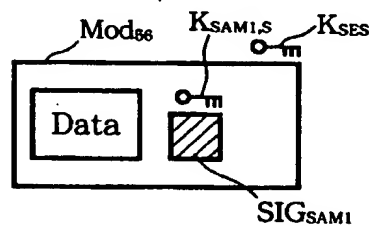
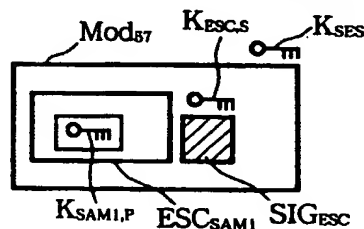


FIG.42F 102 (ESC) → 101 (CP)
(アウト・オブ・バンド)



THIS PAGE BLANK (USPTO)

FIG.43A 101 (CP) → 102 (ESC)
(イン・バンド)

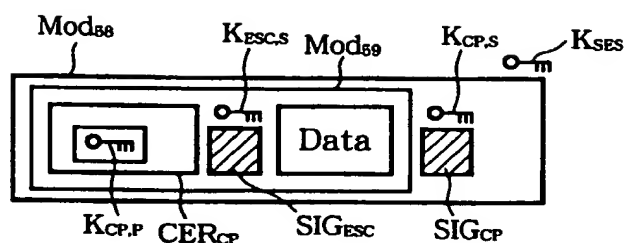


FIG.43B 101 (CP) → 102 (ESC)
(アウト・オブ・バンド)

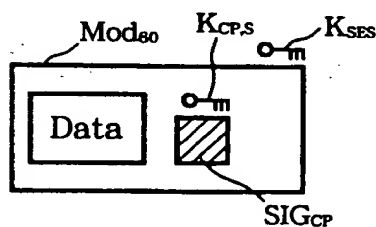


FIG.43C SAM105₁ → 102 (ESC)
(イン・バンド)

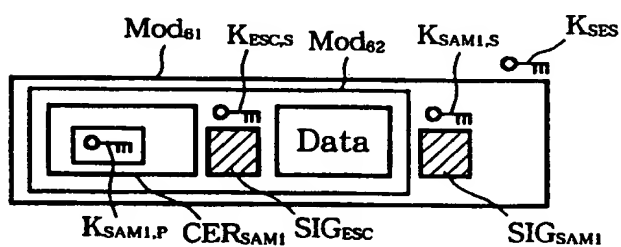
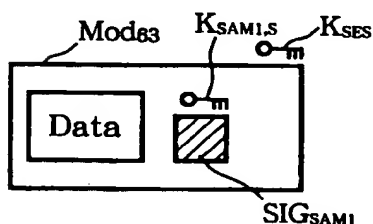


FIG.43D SAM105₁ → 102 (ESC)
(アウト・オブ・バンド)



THIS PAGE BLANK (USPTO)

FIG.44

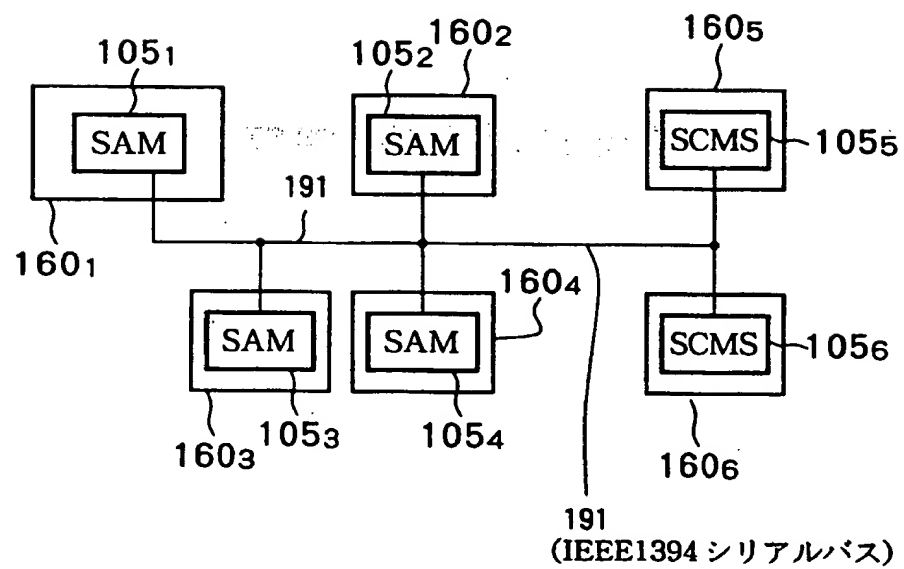




FIG.45

リストを発行したSAMのSAM_ID(Issure_SAM)
SAM登録リストの有効期限
SAM登録数
SAMの接続リスト(SAM_ID)
SAMの決済機能 有/無(Settlement Function)
Revocation_Flag そのSAMがリボークされているか。
各々のSAMの公開鍵

ESC 秘密鍵による署名データ

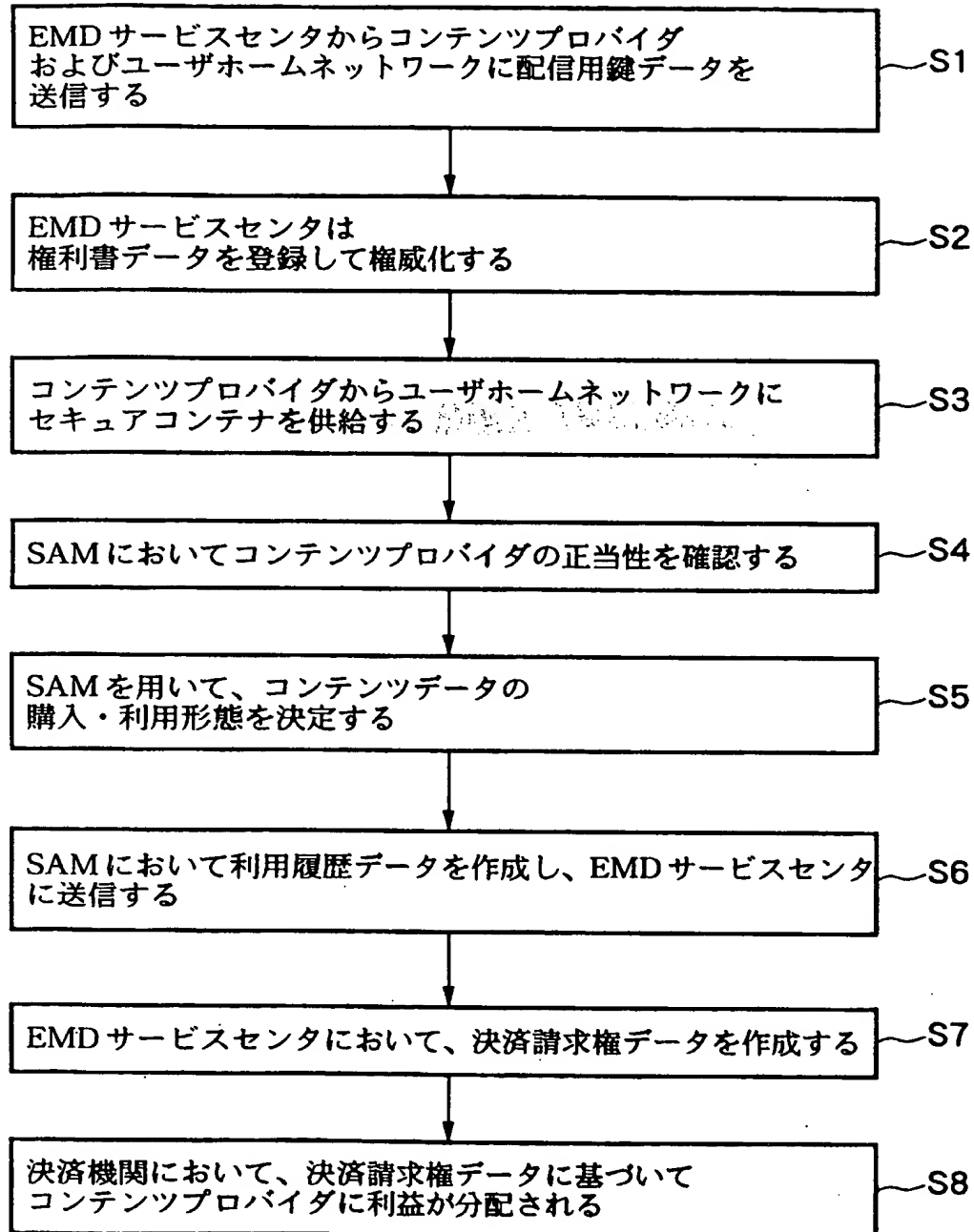
ハッシュ関数

リストを発行したSAMのSAM_ID(Issure_SAM)
Registration Listの有効期限
SAM登録数
SAMの接続リスト(SAM_ID)
SAMの決済機能 有/無(Settlement Function)
Revocation_Flag そのSAMがリボークされているか。
各々のSAMの公開鍵

SAM登録リスト

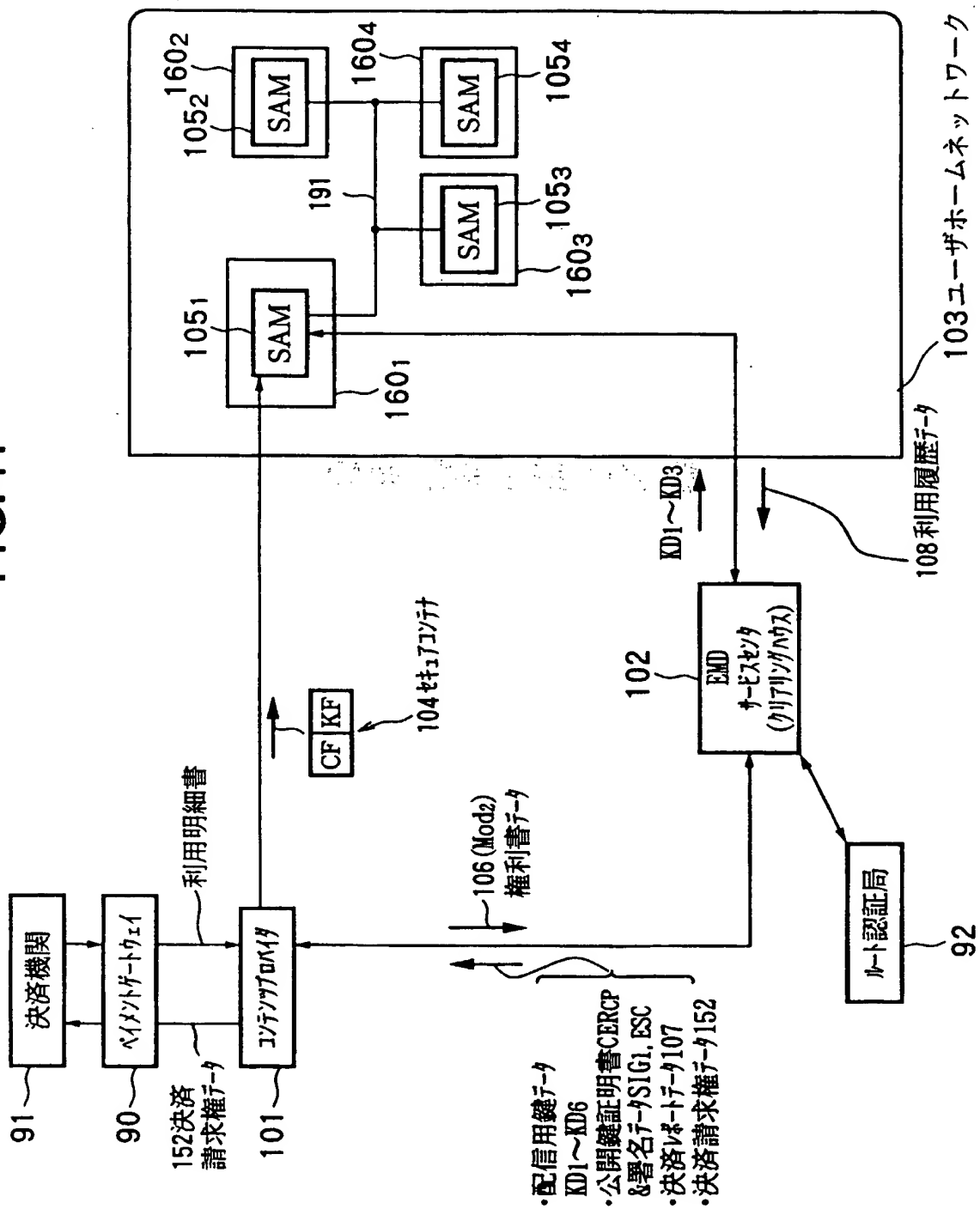
THIS PAGE BLANK (USPTO)

FIG.46



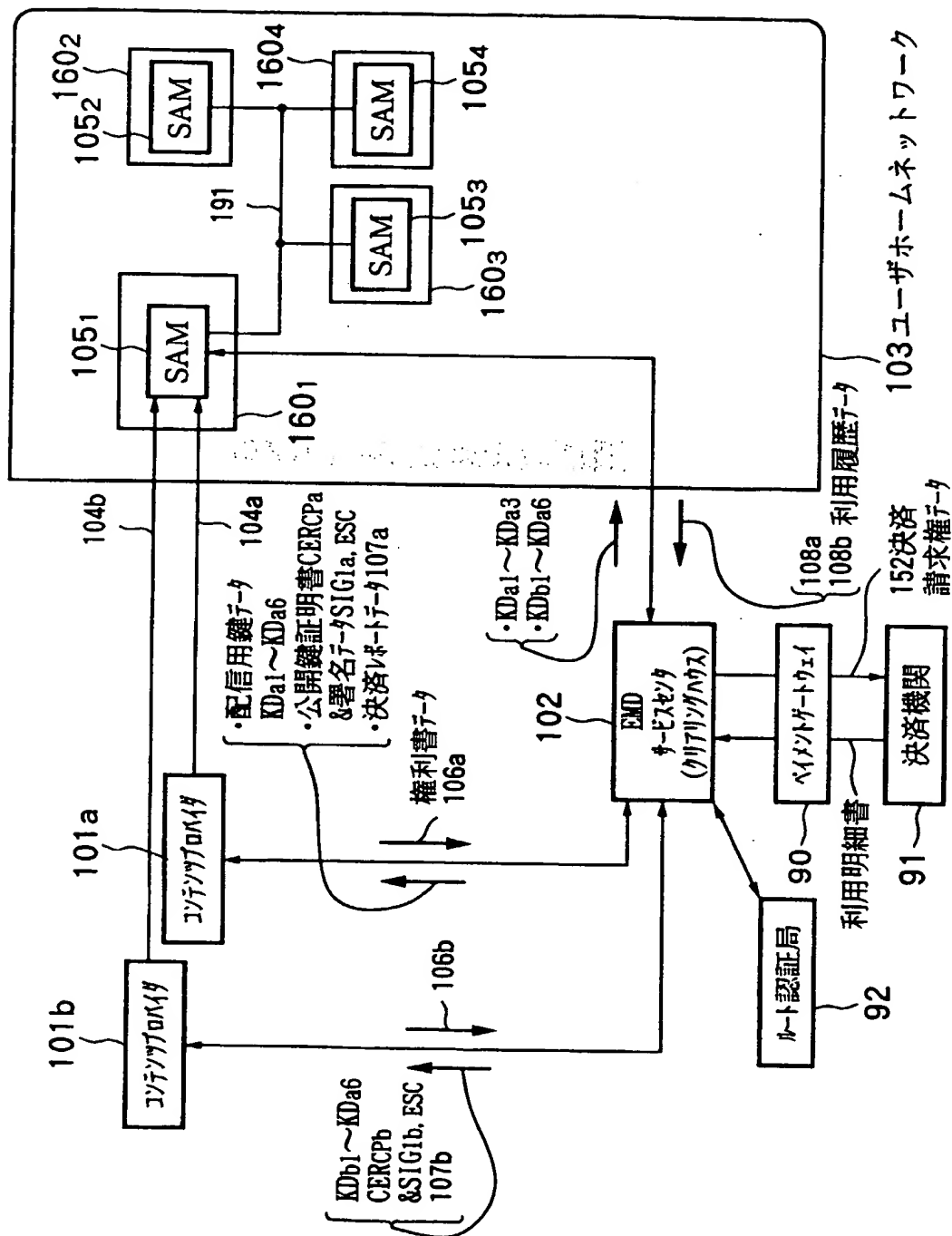
THIS PAGE BLANK (USPTO)

FIG. 47



THIS PAGE BLANK (USPTO)

FIG. 48

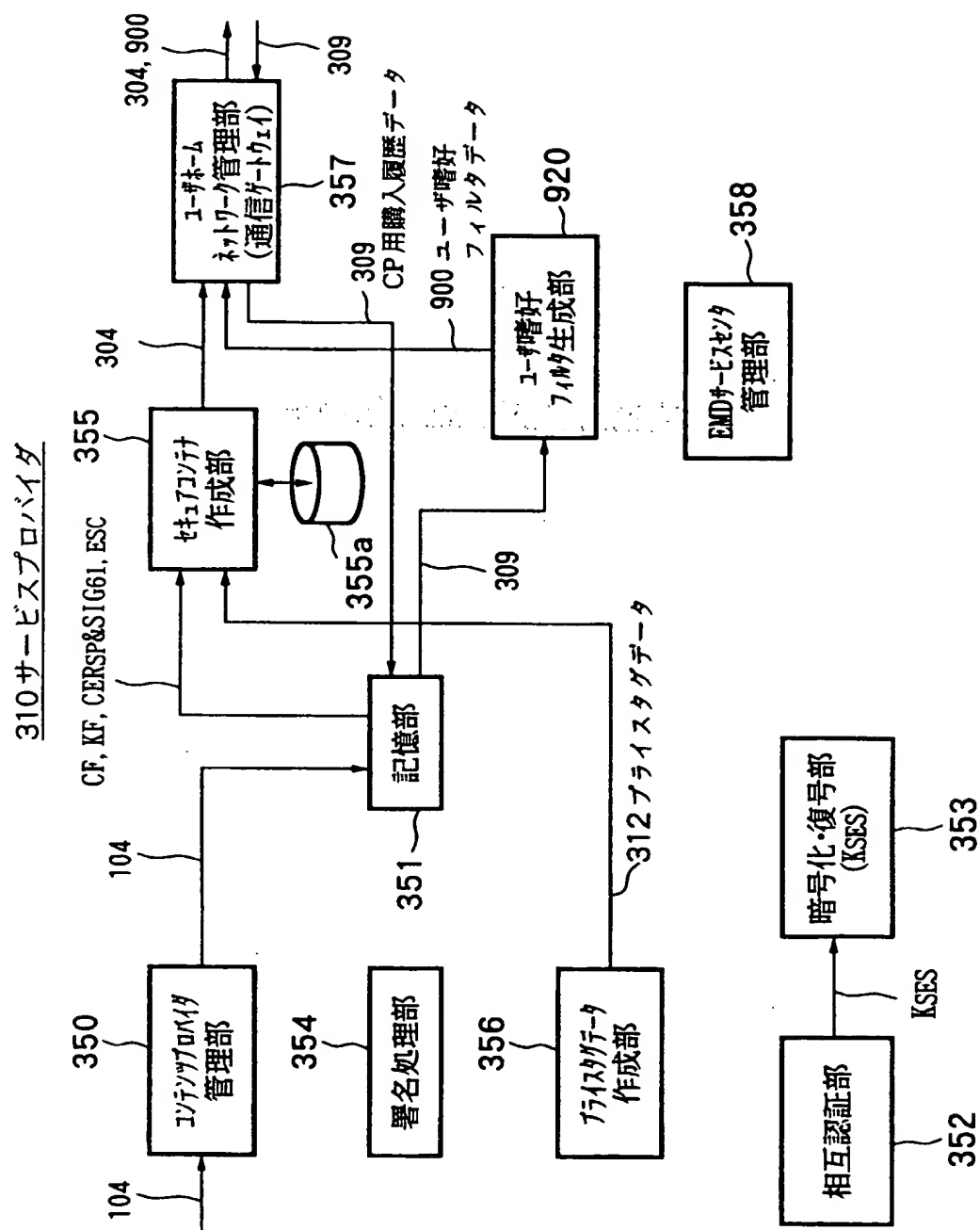


THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

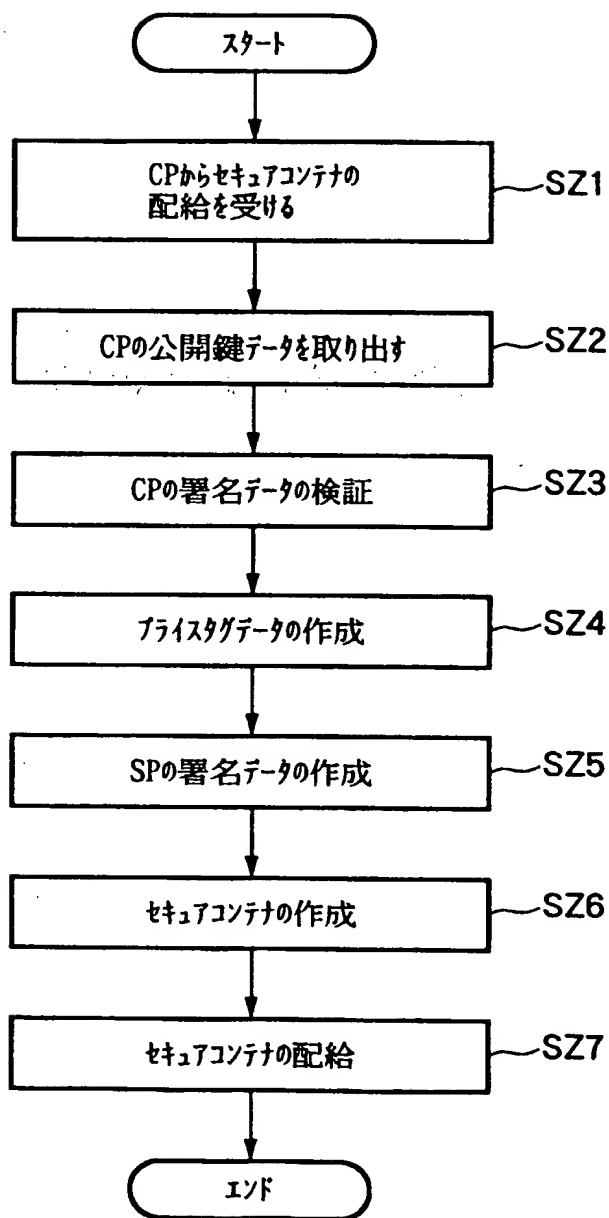
THIS PAGE BLANK (USPTO)

FIG. 51



THIS PAGE BLANK (USPTO)

FIG.52



THIS PAGE BLANK (USPTO)

304セキユアコンテナ

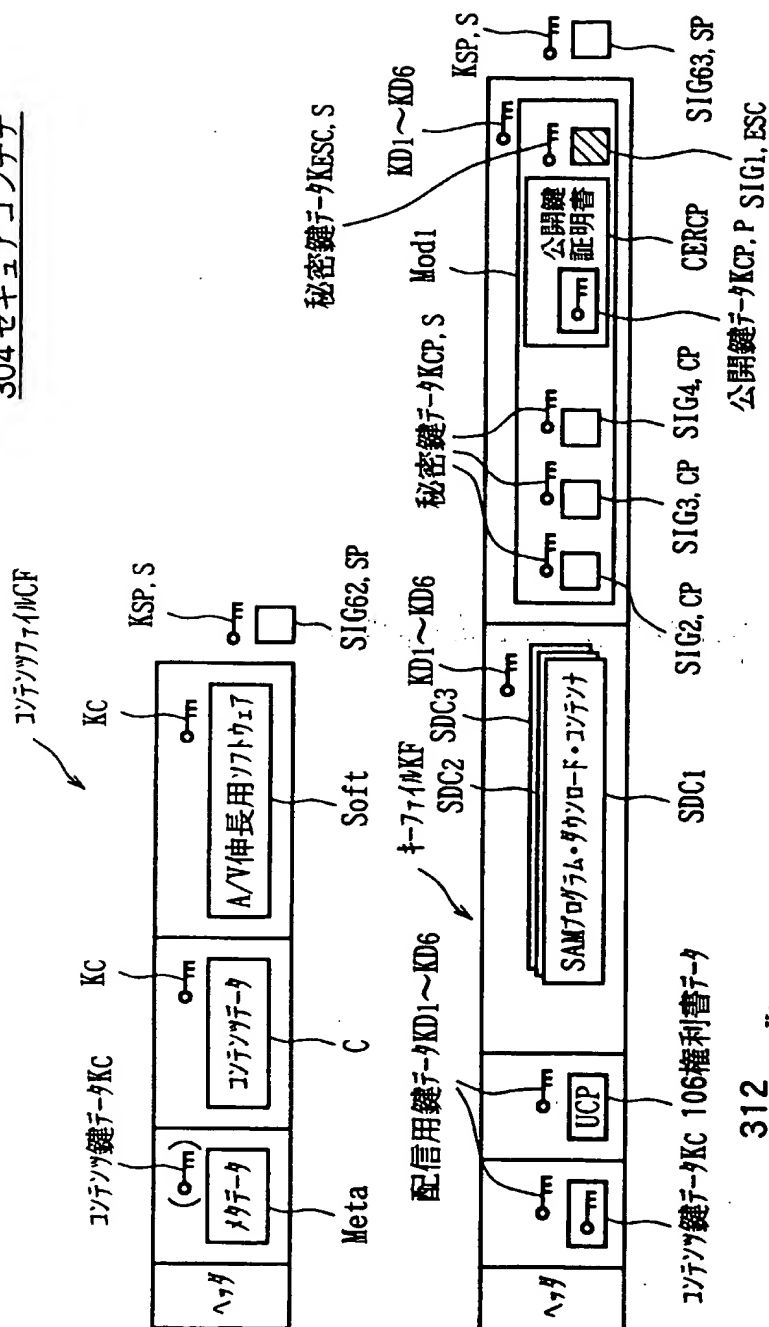


FIG. 53A

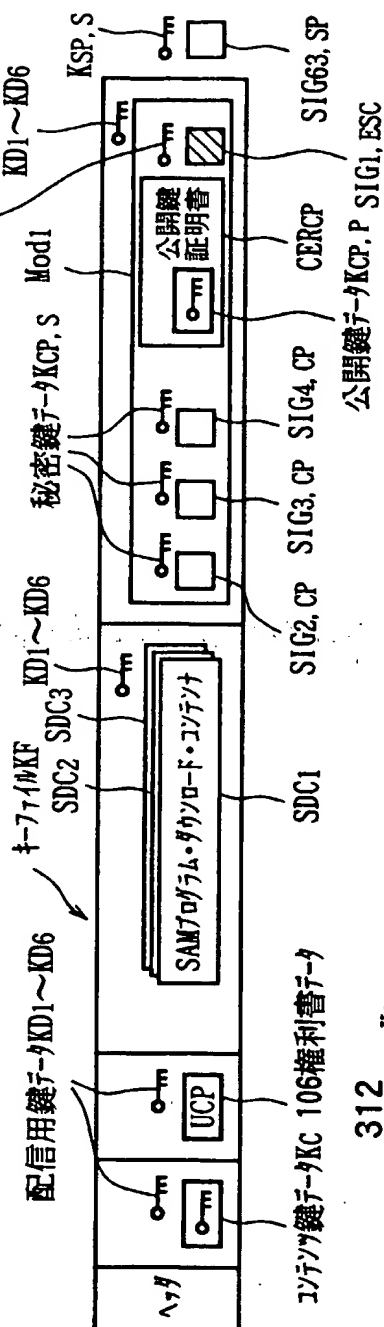


FIG. 53B

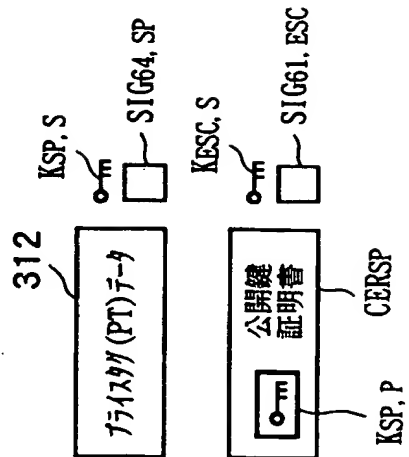


FIG. 53C

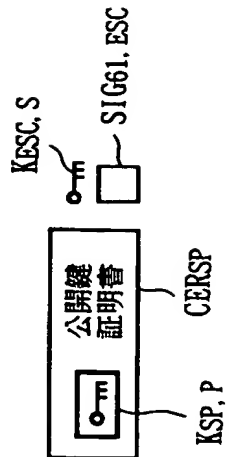
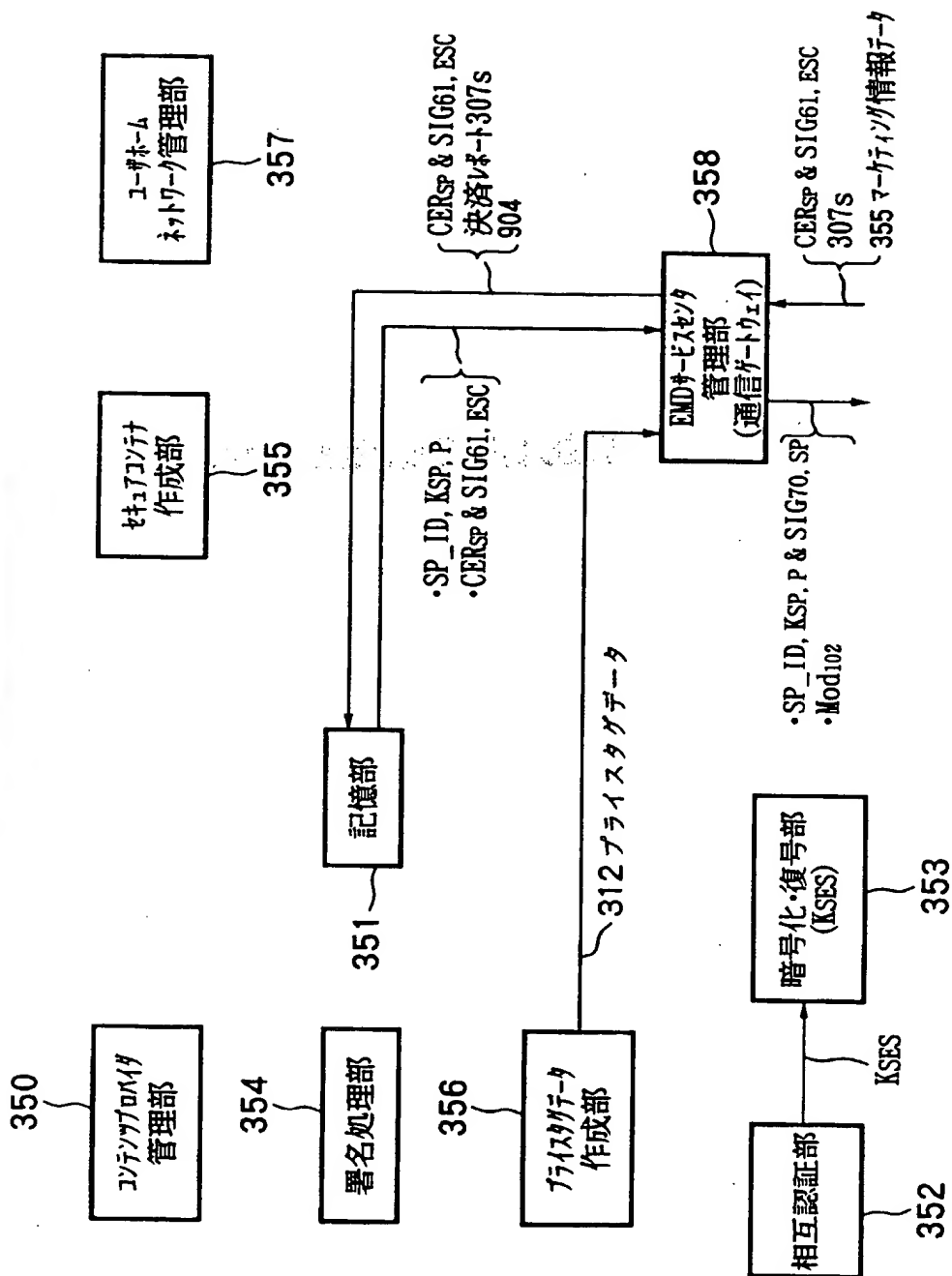


FIG. 53D

THIS PAGE BLANK (USPTO)

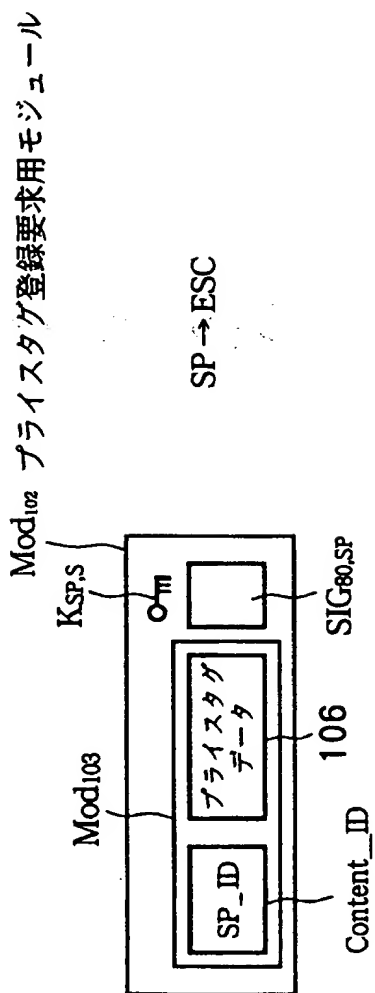
FIG.54

310 サービスプロバイダ



THIS PAGE BLANK (USPTO)

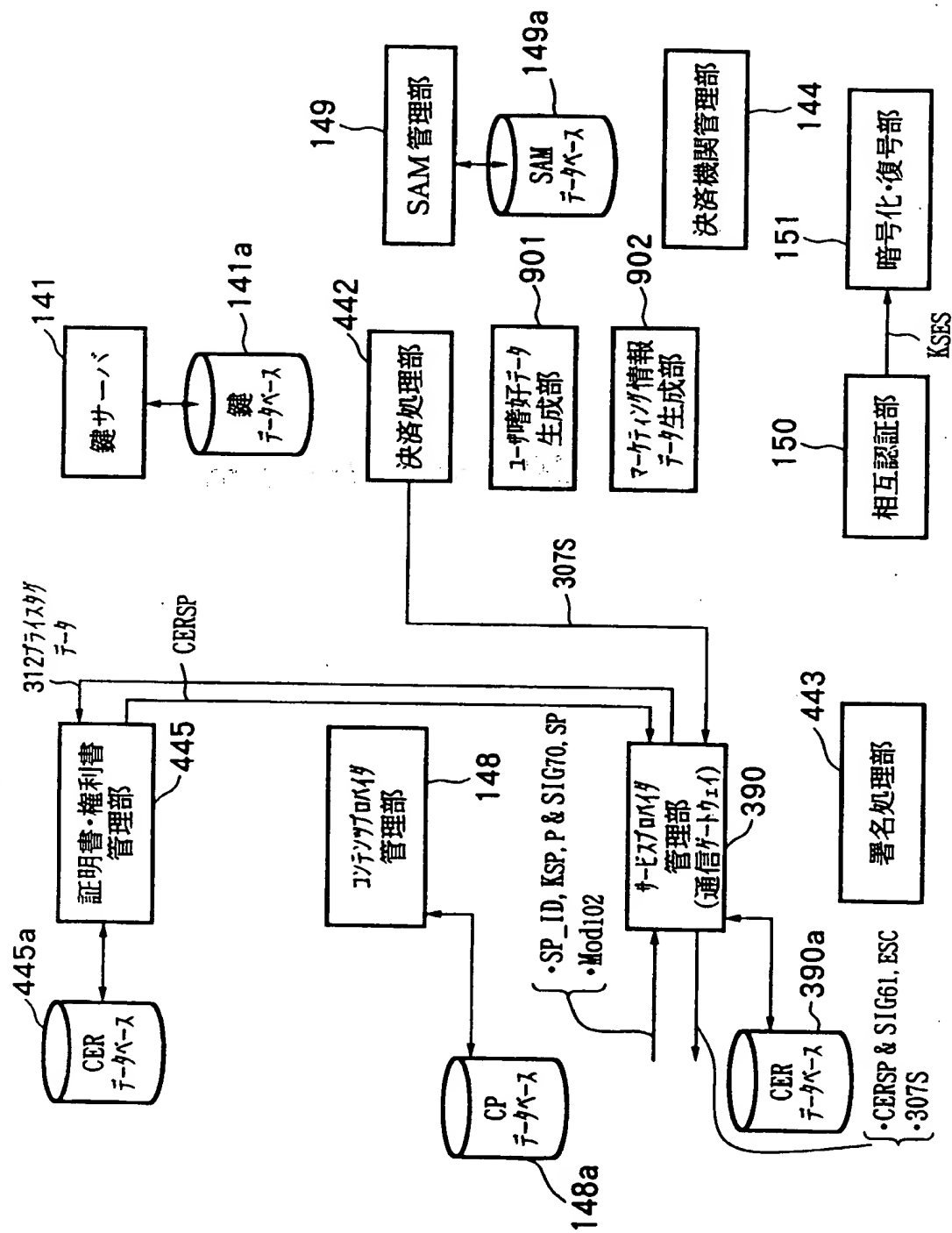
FIG.55



THIS PAGE BLANK (USPTO)

FIG.56

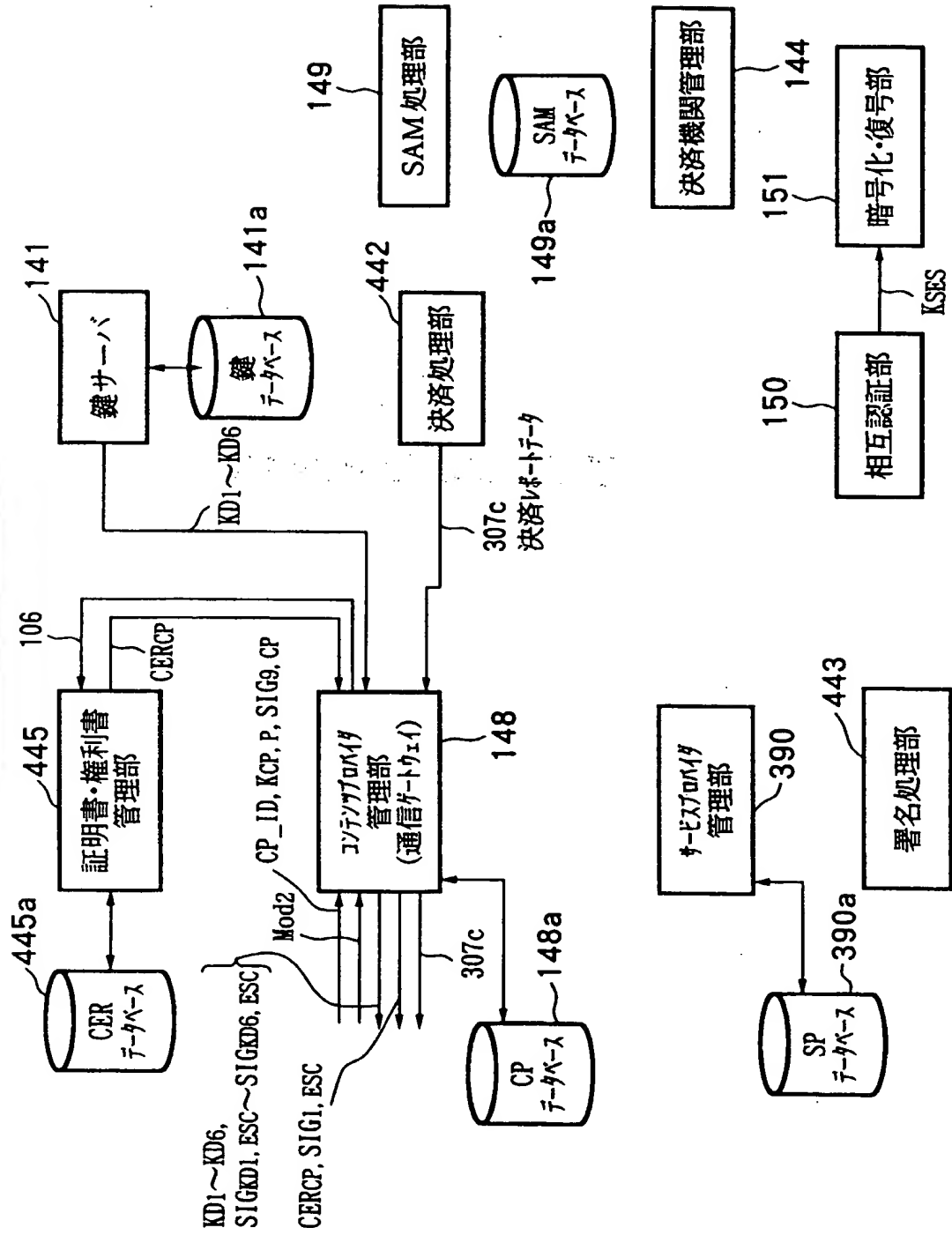
302EMD サービスセンタ



THIS PAGE BLANK (USPTO)

FIG.57

EMD サービスセンタ 302



THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

FIG.59

利用履歴データ 308 の内容

識別子 Content_ID

識別子 CP_ID

識別子 SP_ID

コンテンツデータ C の信号諸元データ

コンテンツデータ C の圧縮方法

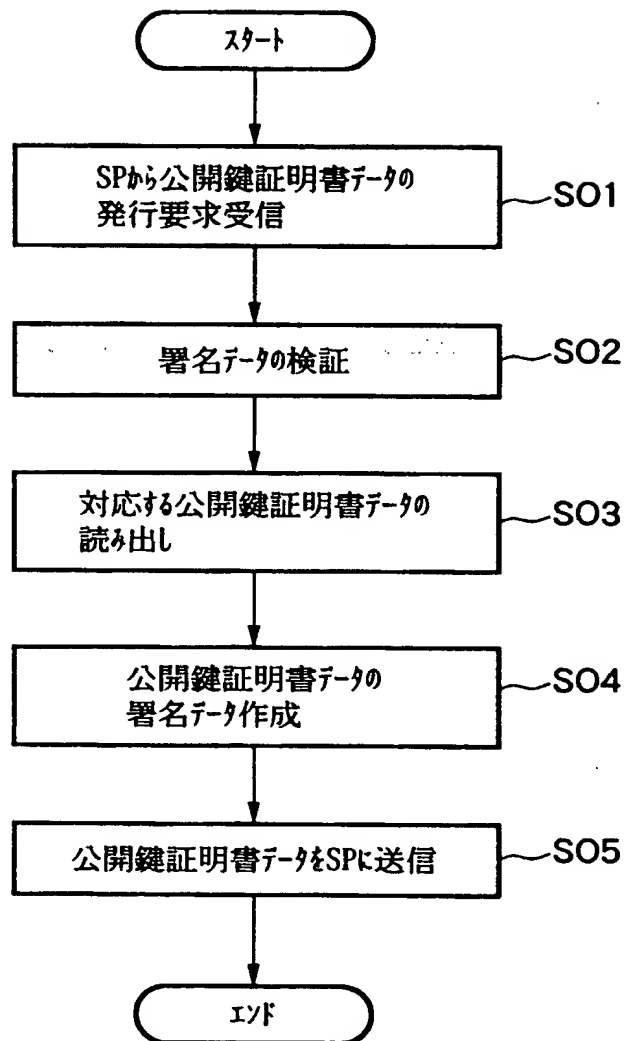
記録媒体の識別子 Media_ID

識別子 SAM_ID、

ユーザの USER_ID

THIS PAGE BLANK (USPTO)

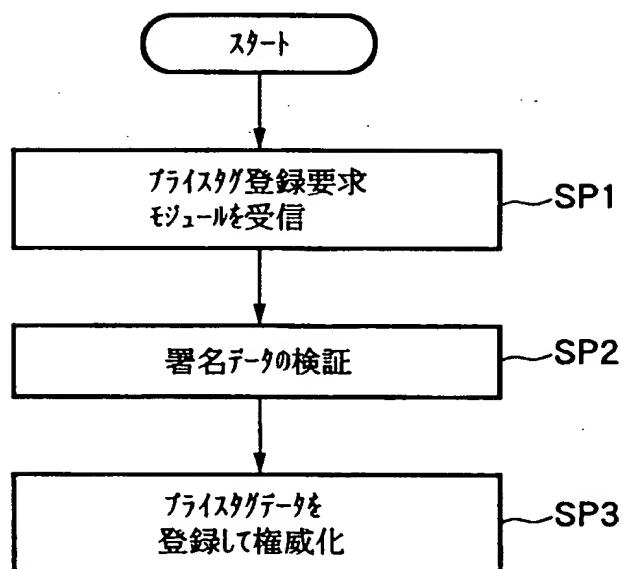
FIG.60



SPからの公開鍵証明書データの発行要求に応じたESCの処理

THIS PAGE BLANK (USPTO)
THIS PAGE BLANK (USPTO)

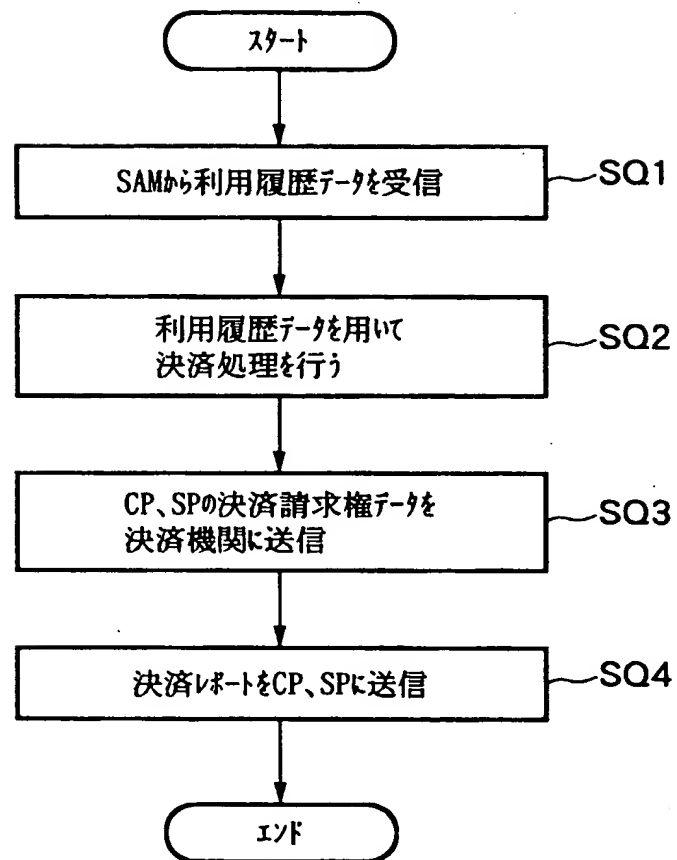
FIG.61



ESCにおけるプライスタグデータの登録処理

THIS PAGE BLANK (USPTO)

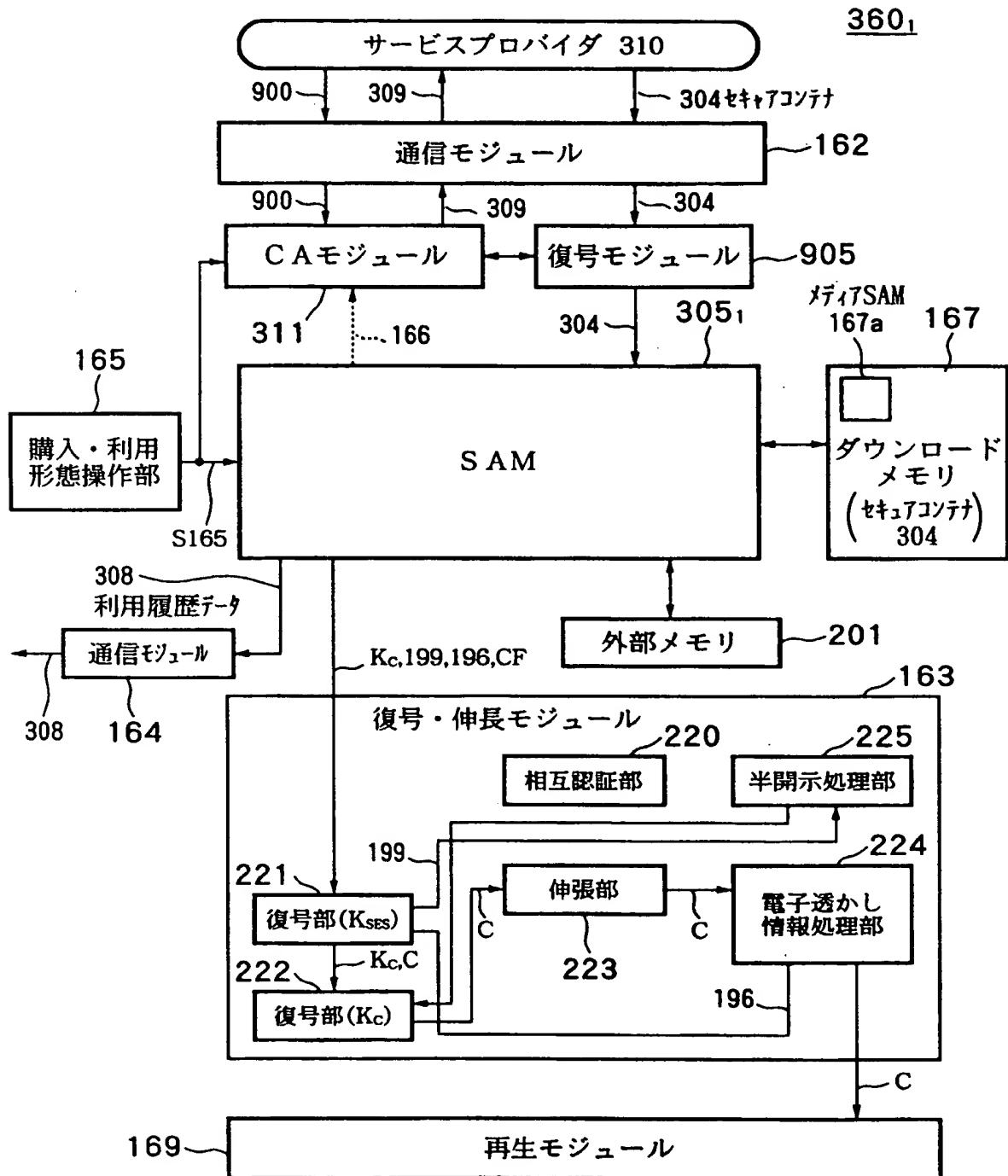
FIG.62



ESCにおける決済処理

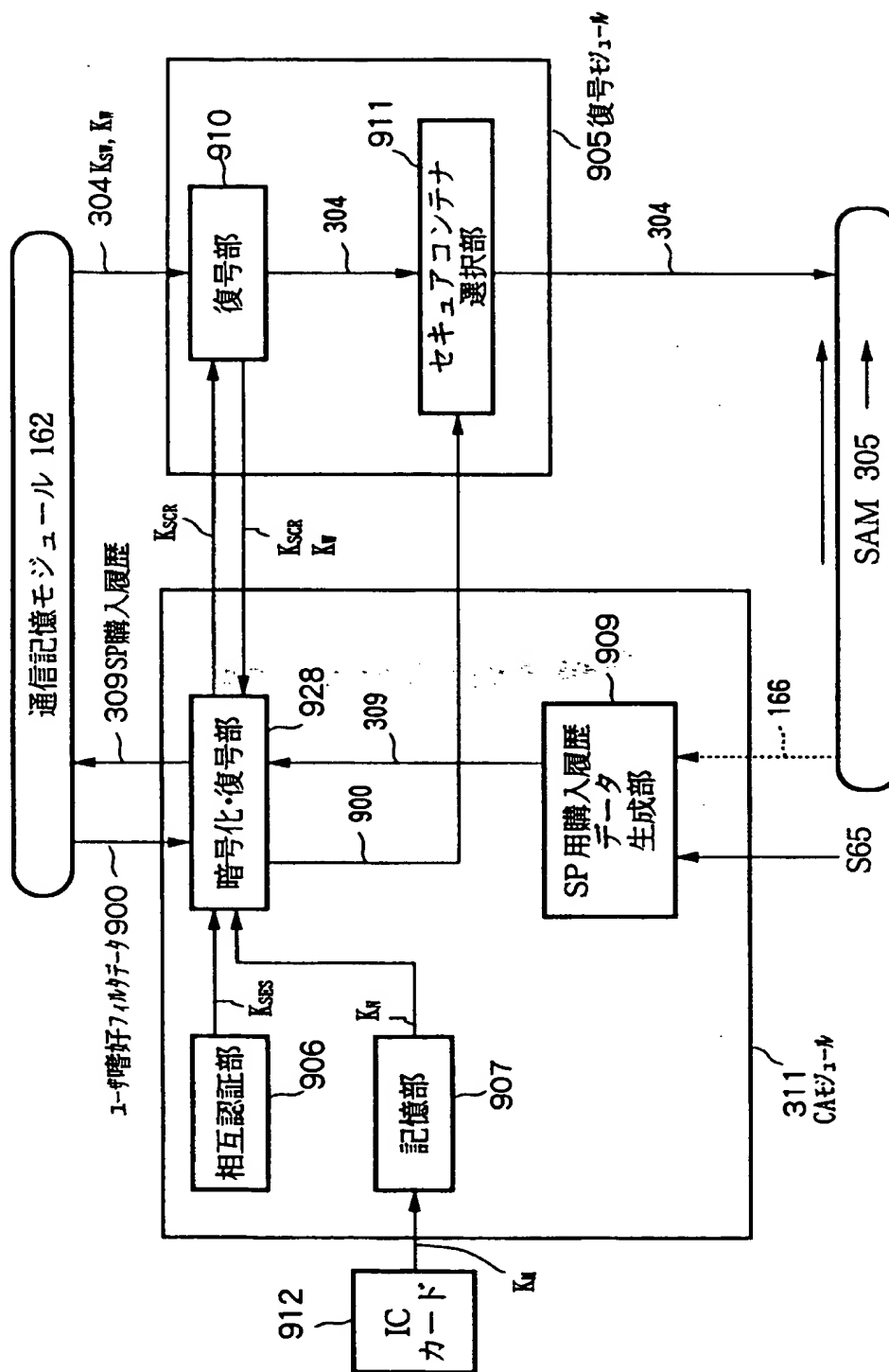
THIS PAGE BLANK (USPTO)

FIG.63



THIS PAGE BLANK (USPTO)

FIG.64



THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

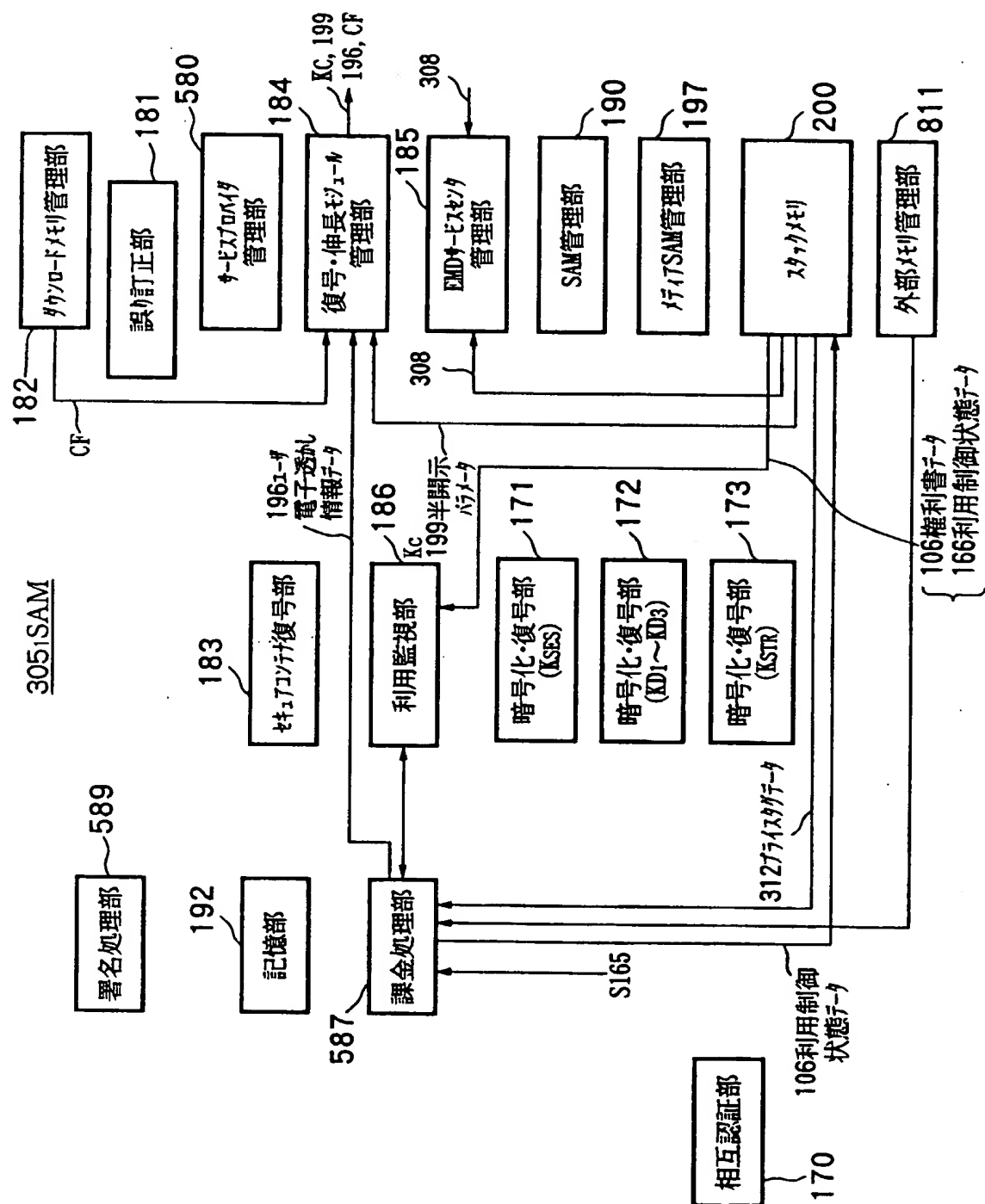
FIG.66

スタックメモリ 200 の記憶データ

コンテンツ鍵データ K_c
権利書データ (UCP) 106
不揮発性メモリ 201 のロック鍵データ K_{Loc}
コンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP}
サービスプロバイダ 301 の公開鍵証明書データ CER_{SP}
利用制御情状態データ (UCS) 166
SAM プログラム・ダウンロード・コンテナ SD₁~SDC₃
プライスタグデータ 312

THIS PAGE BLANK (USPTO)

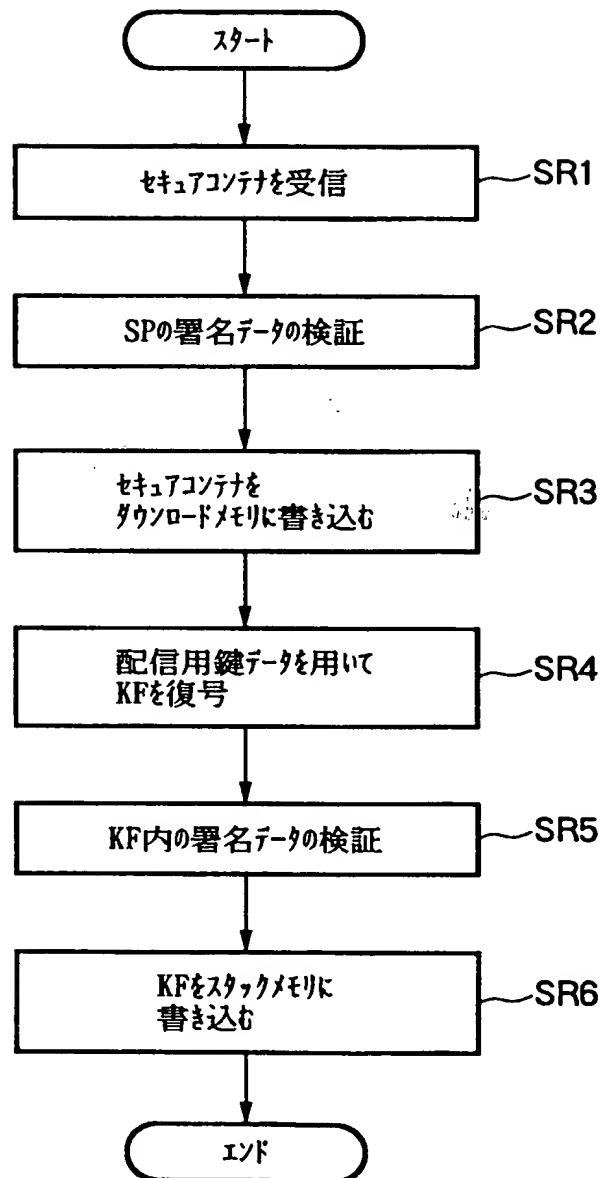
FIG. 67

3051SAM

THIS PAGE BLANK (USPTO)

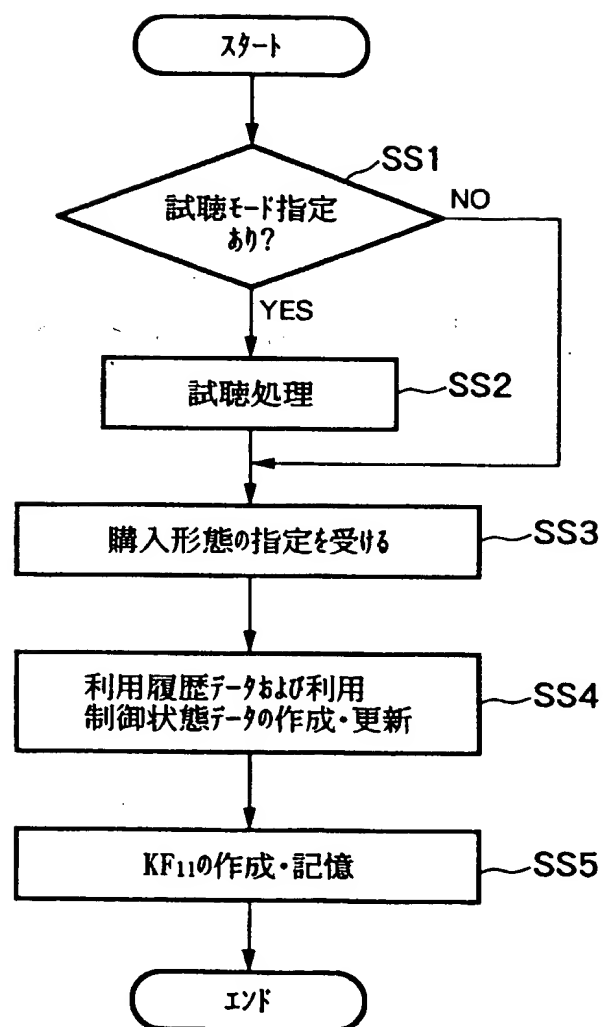
THIS PAGE BLANK (USPTO)

FIG.68

SAMにおけるKFの復号処理

THIS PAGE BLANK (USPTO)

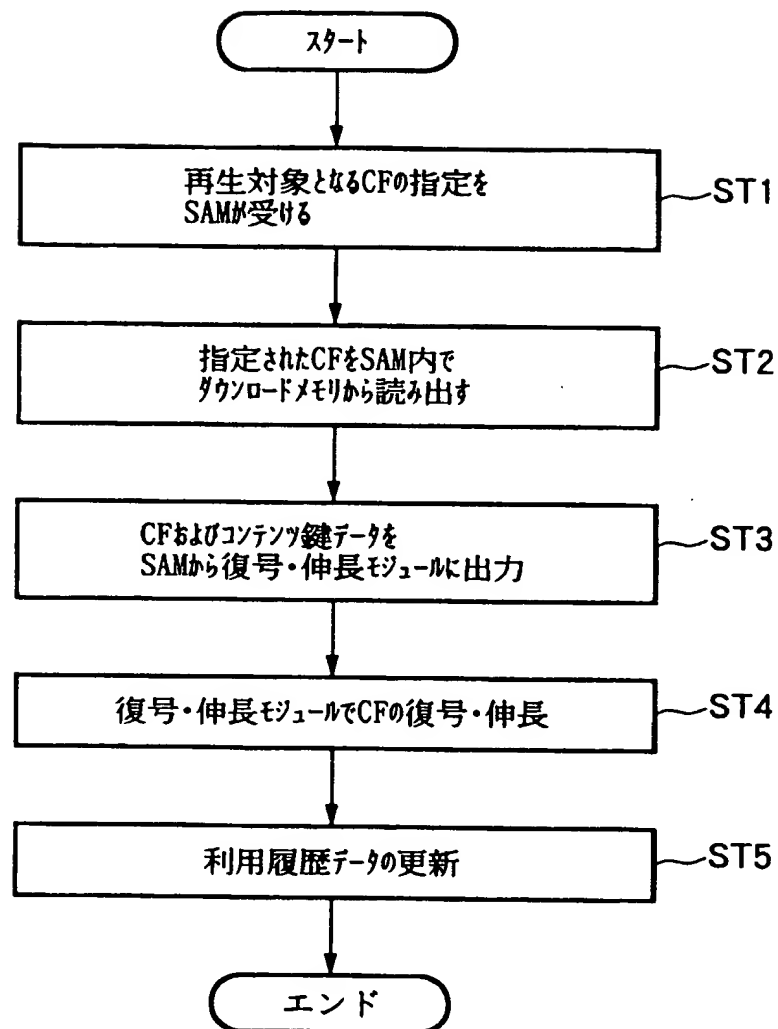
FIG.69



SAMにおけるセキュアコンテナの購入形態決定処理

THIS PAGE BLANK (USPTO)

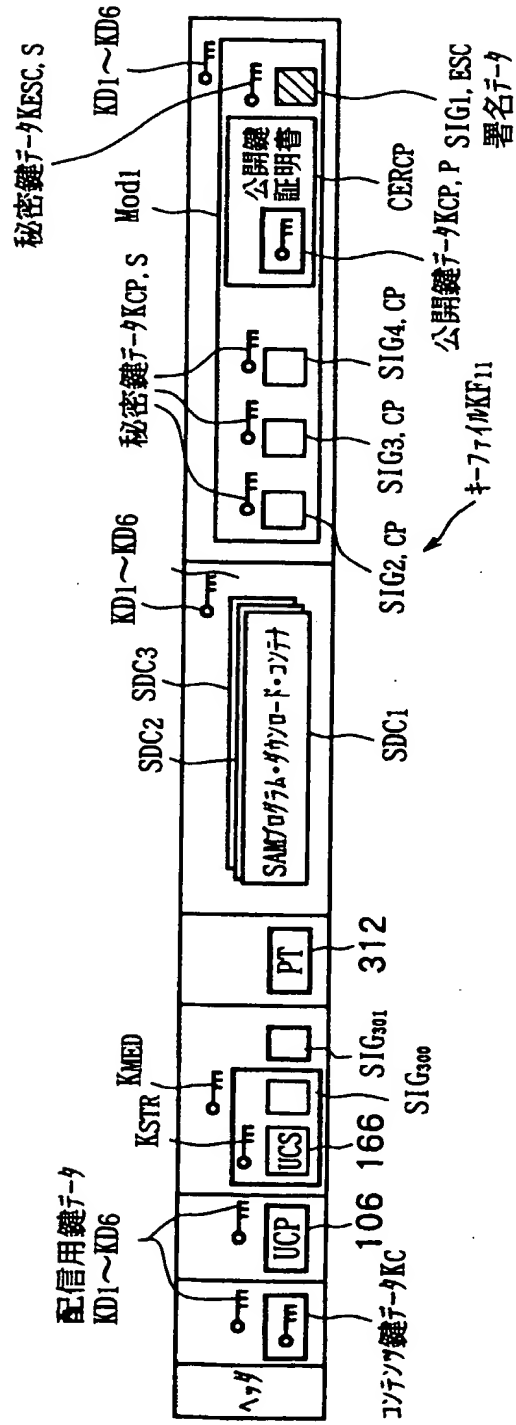
FIG.70



コンテンツデータの再生処理

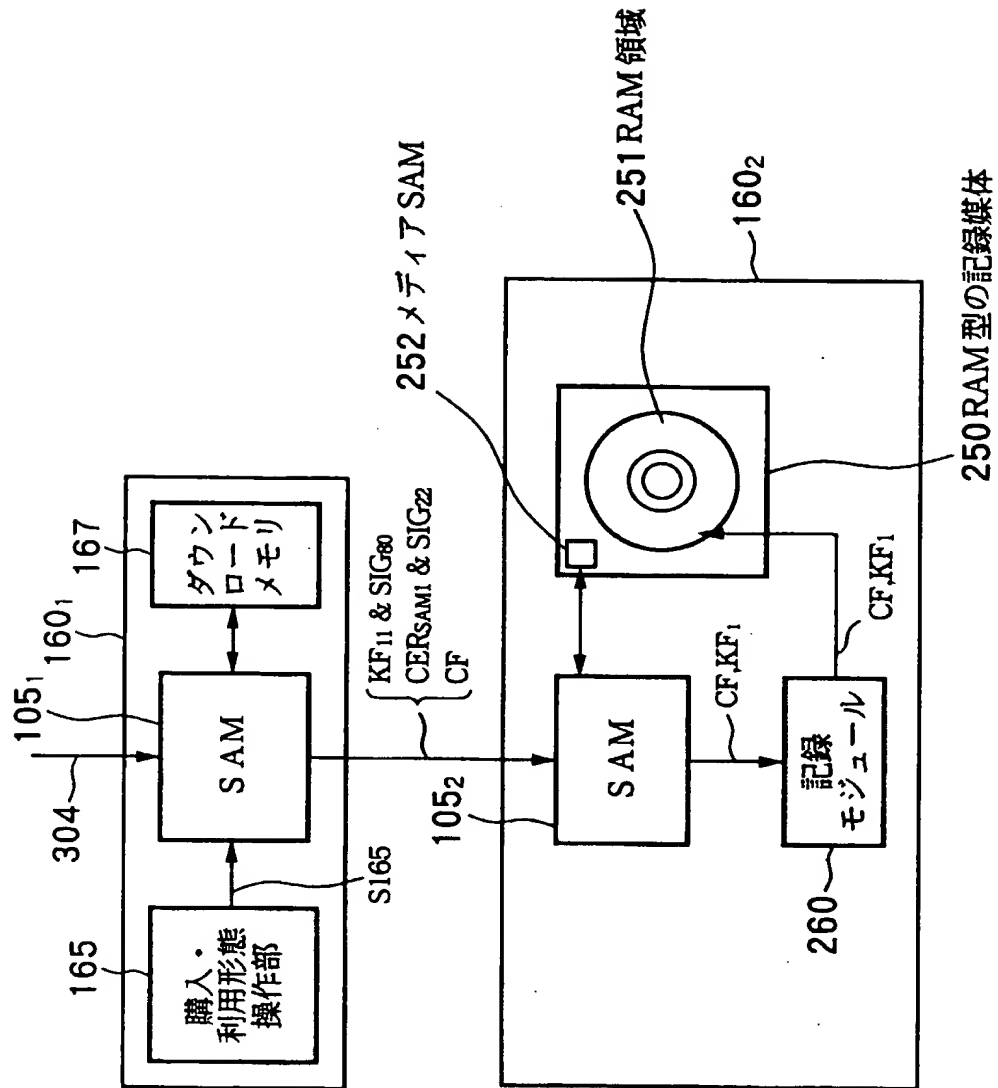
THIS PAGE BLANK (USPTO)

FIG.71



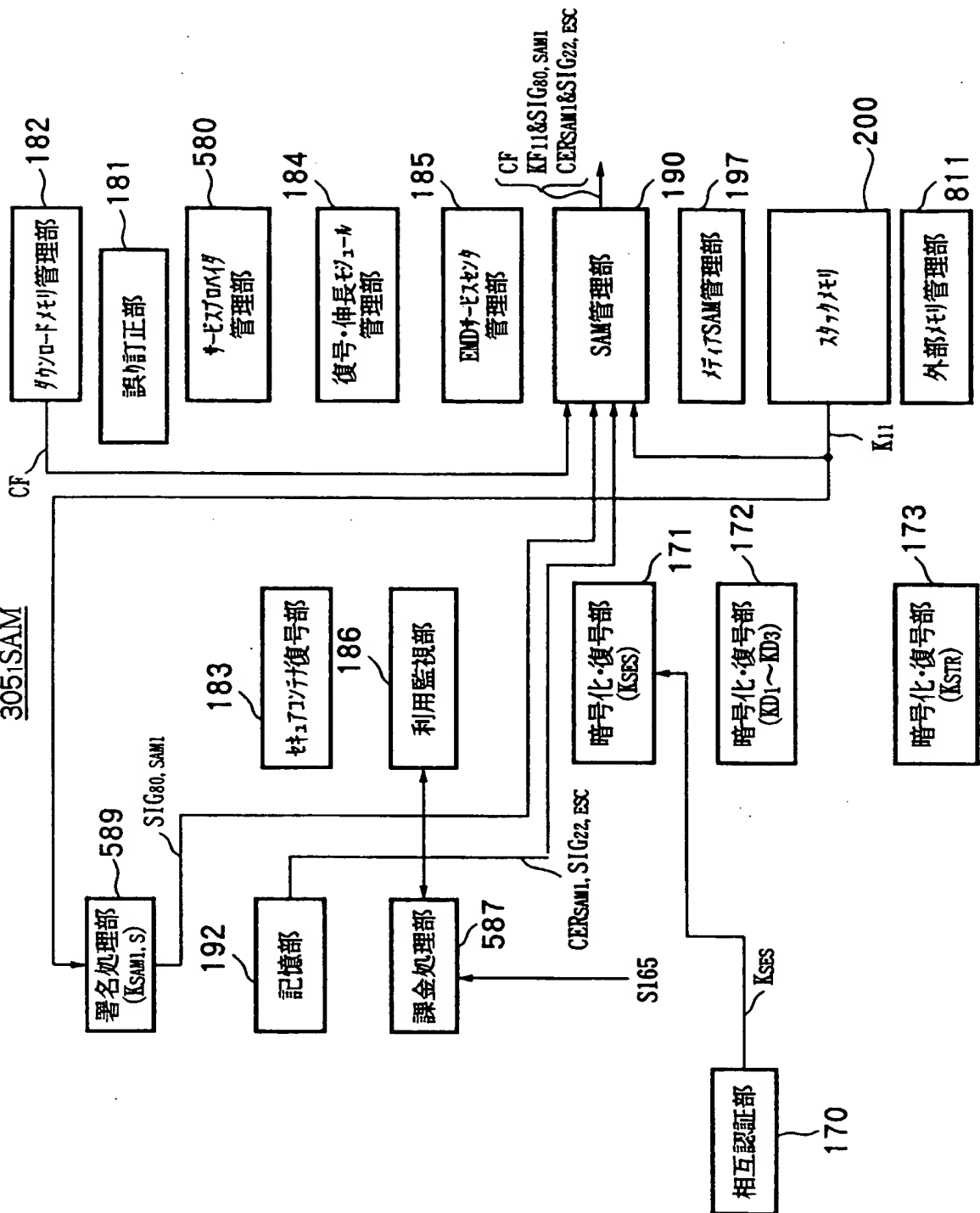
THIS PAGE BLANK (USPTO)

FIG.72



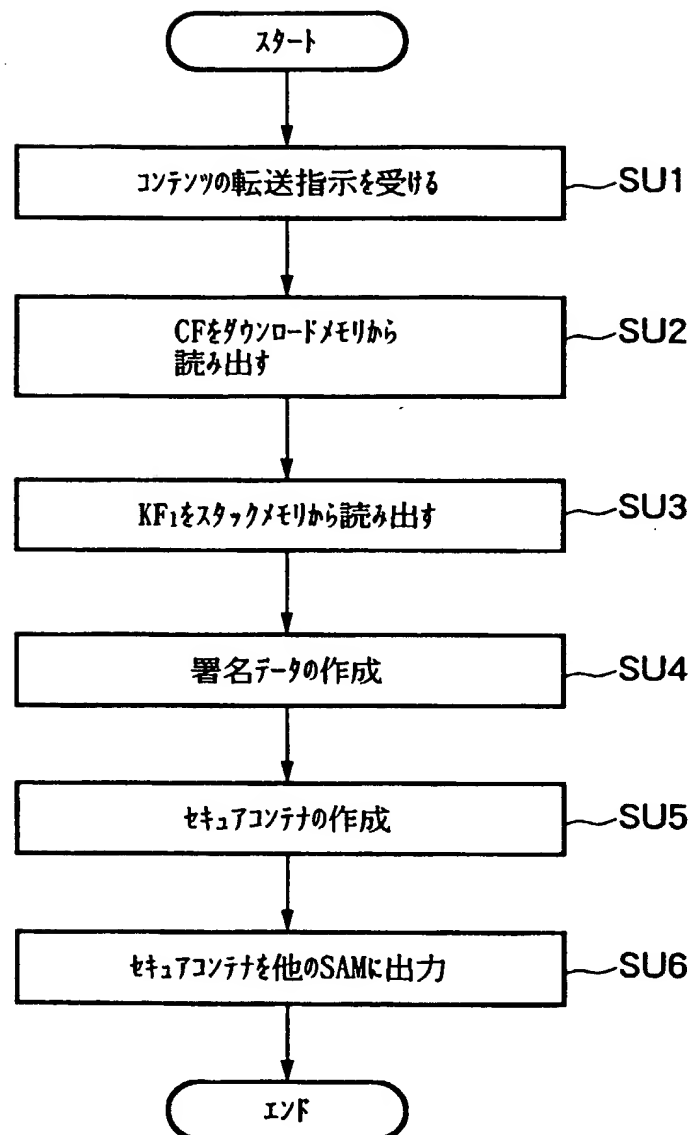
THIS PAGE BLANK (USPTO)

FIG. 73

3051SAM

THIS PAGE BLANK (USPTO)

FIG.74



購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

THIS PAGE BLANK (USPTO)

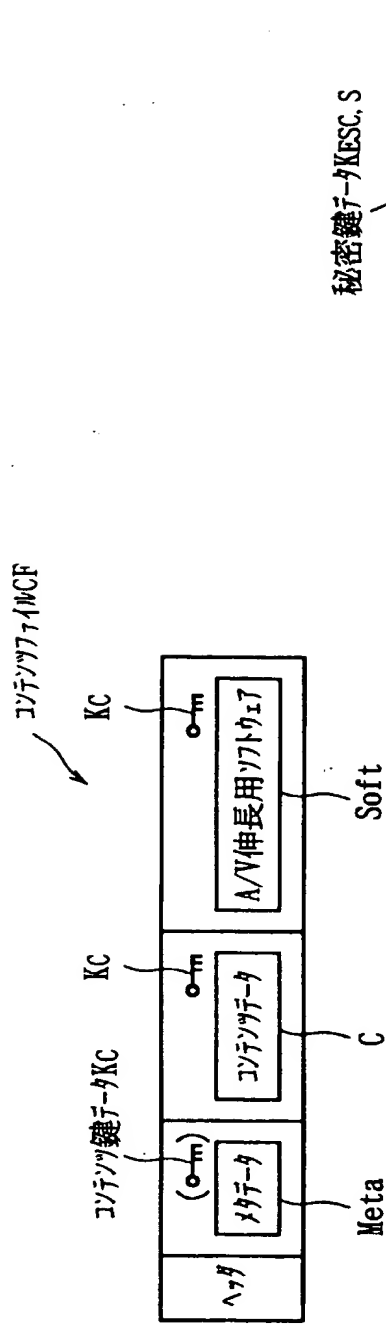


FIG. 75A

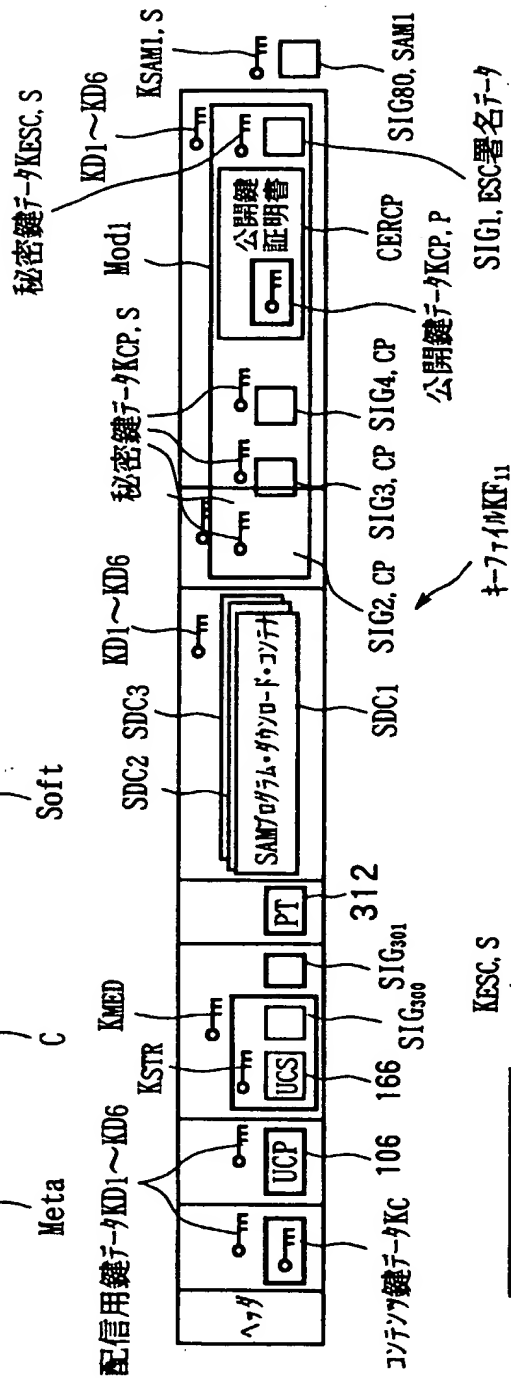


FIG. 75B

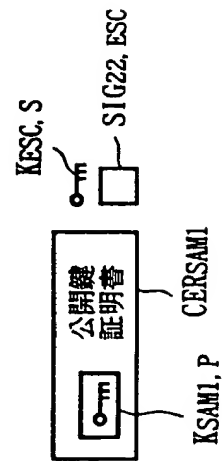
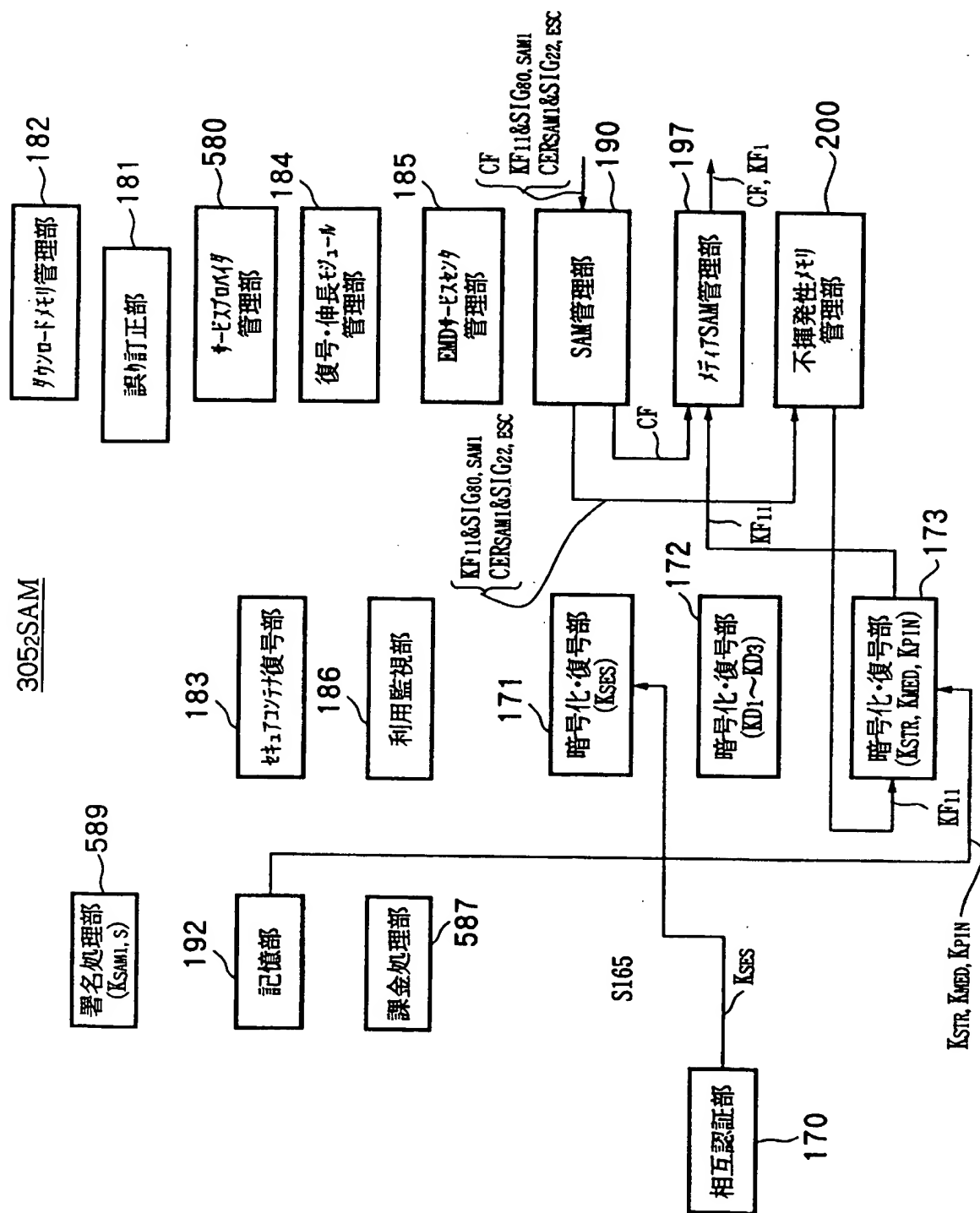


FIG. 75C

THIS PAGE BLANK (USPTO)

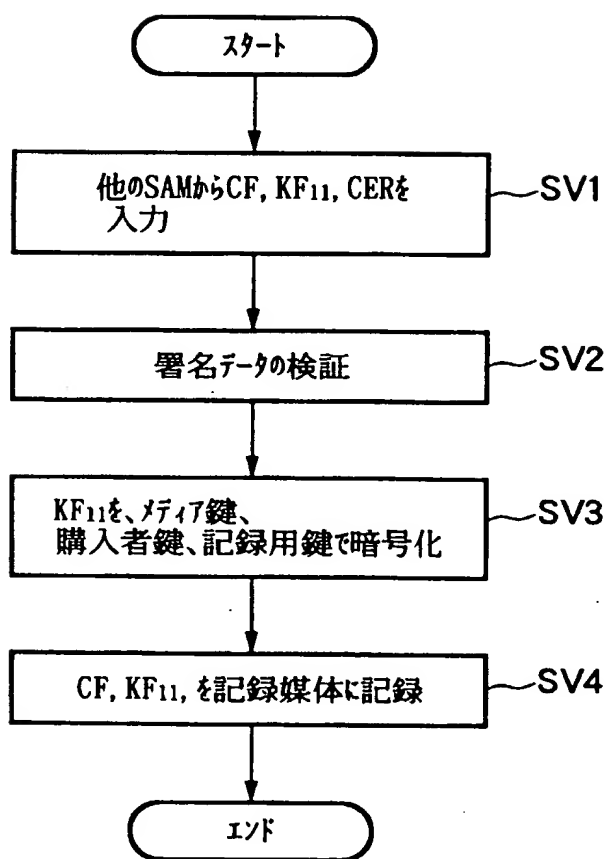
FIG.76

3052SAM



THIS PAGE BLANK (USPTO)

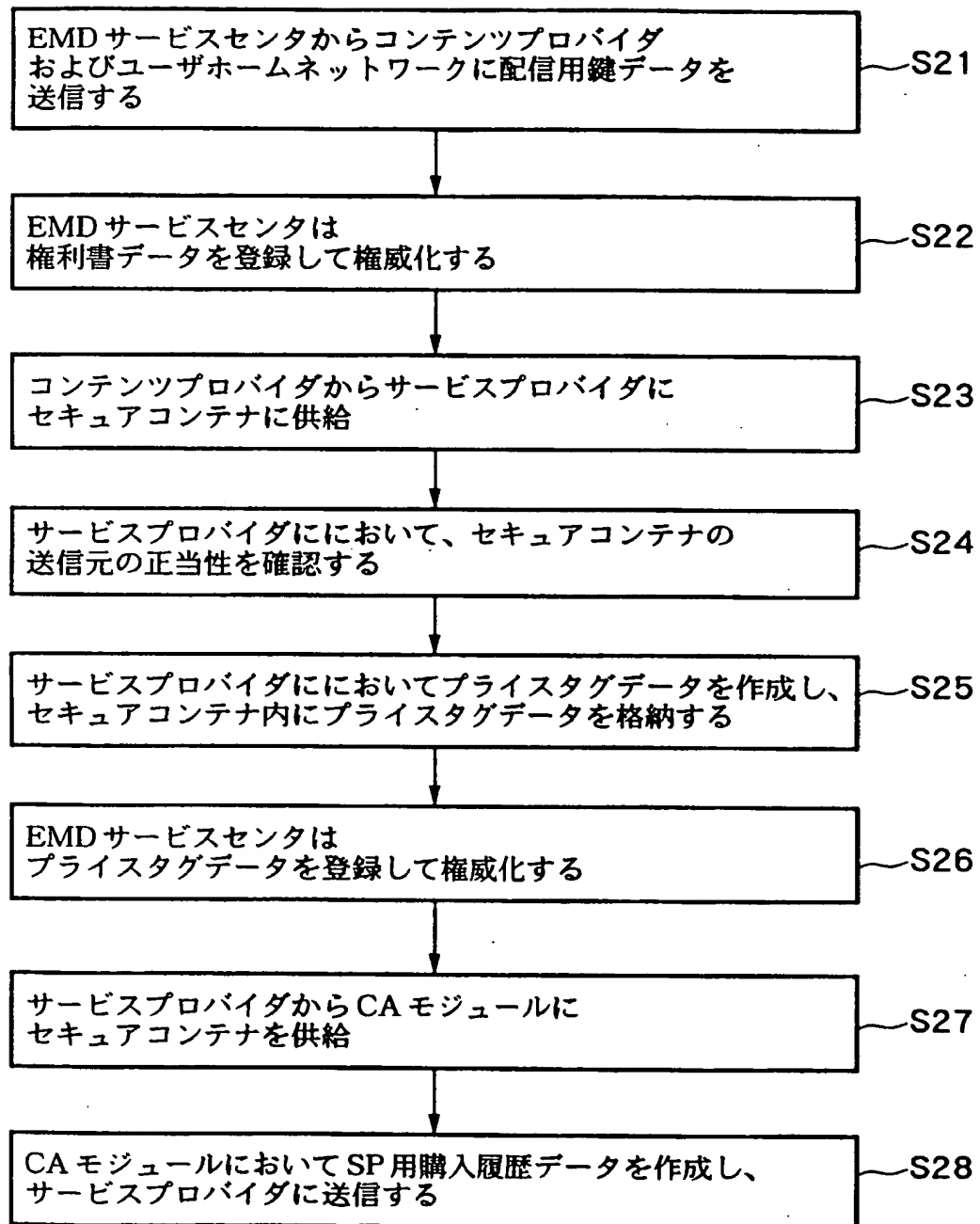
FIG.77



他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

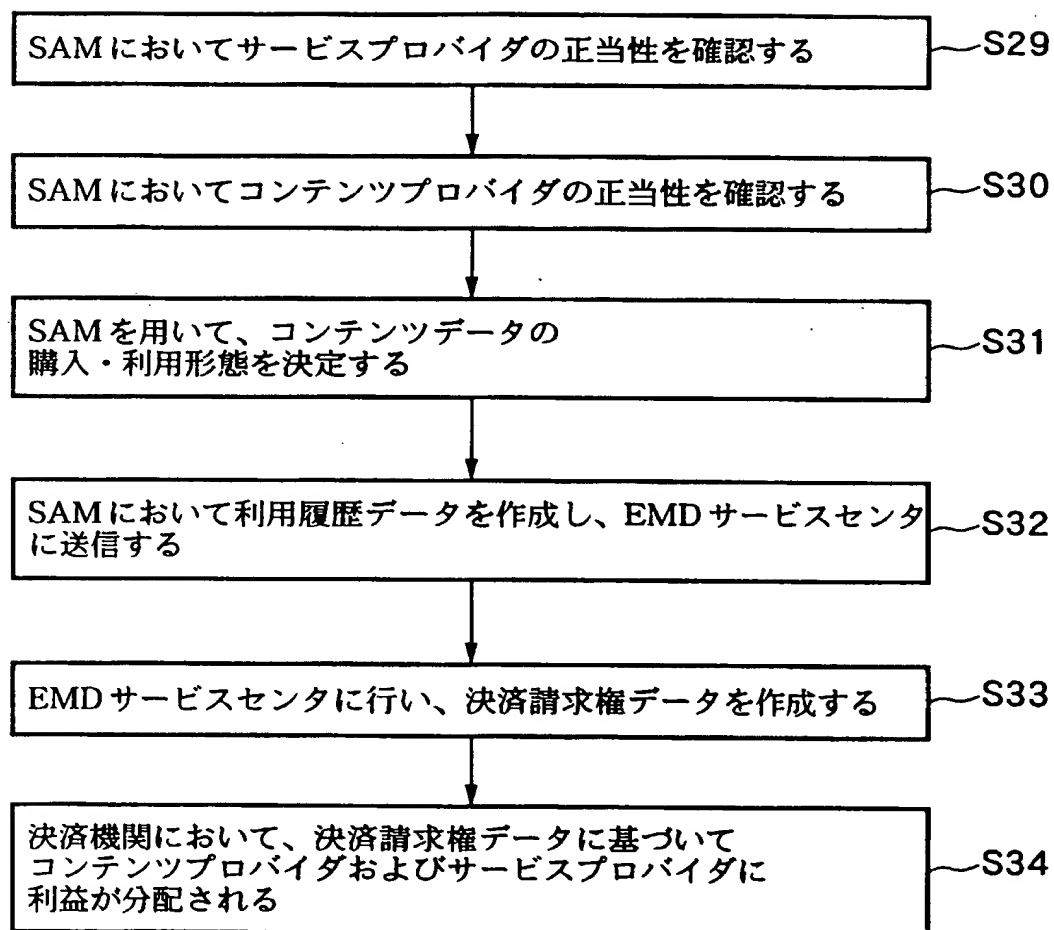
THIS PAGE BLANK (USPTO)

FIG.78



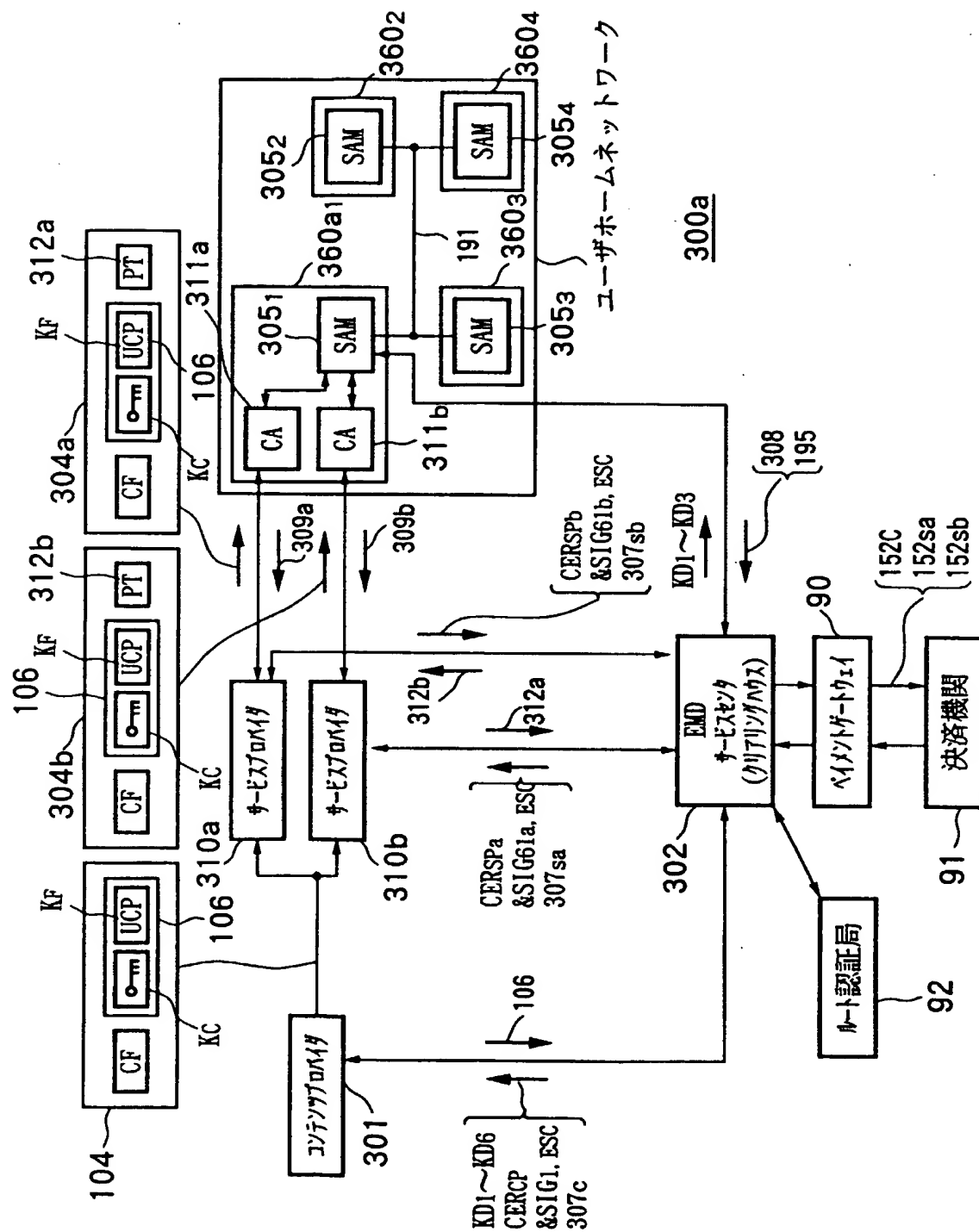
THIS PAGE BLANK (USPTO)

FIG.79



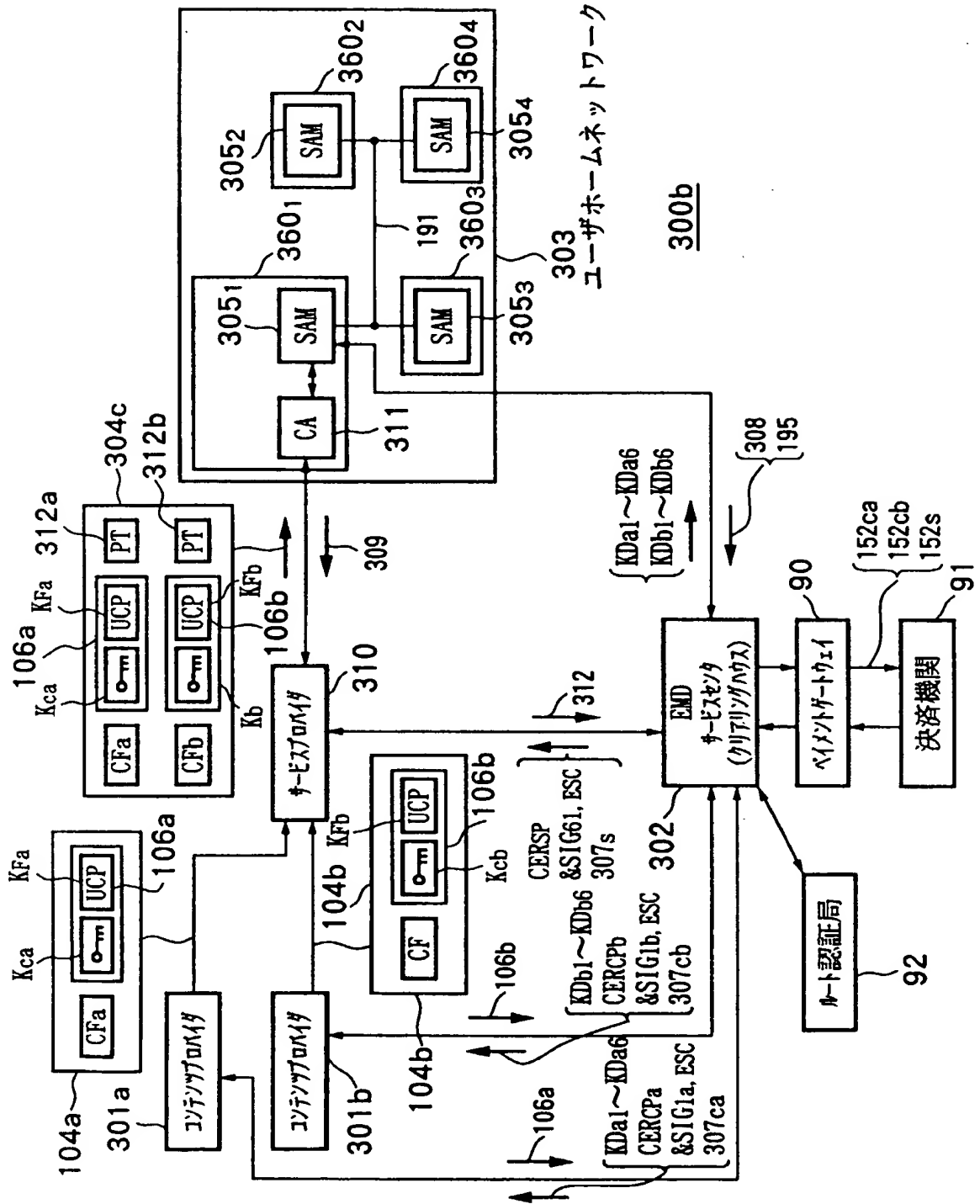
THIS PAGE BLANK (USPTO)

FIG. 80



THIS PAGE BLANK (USPTO)

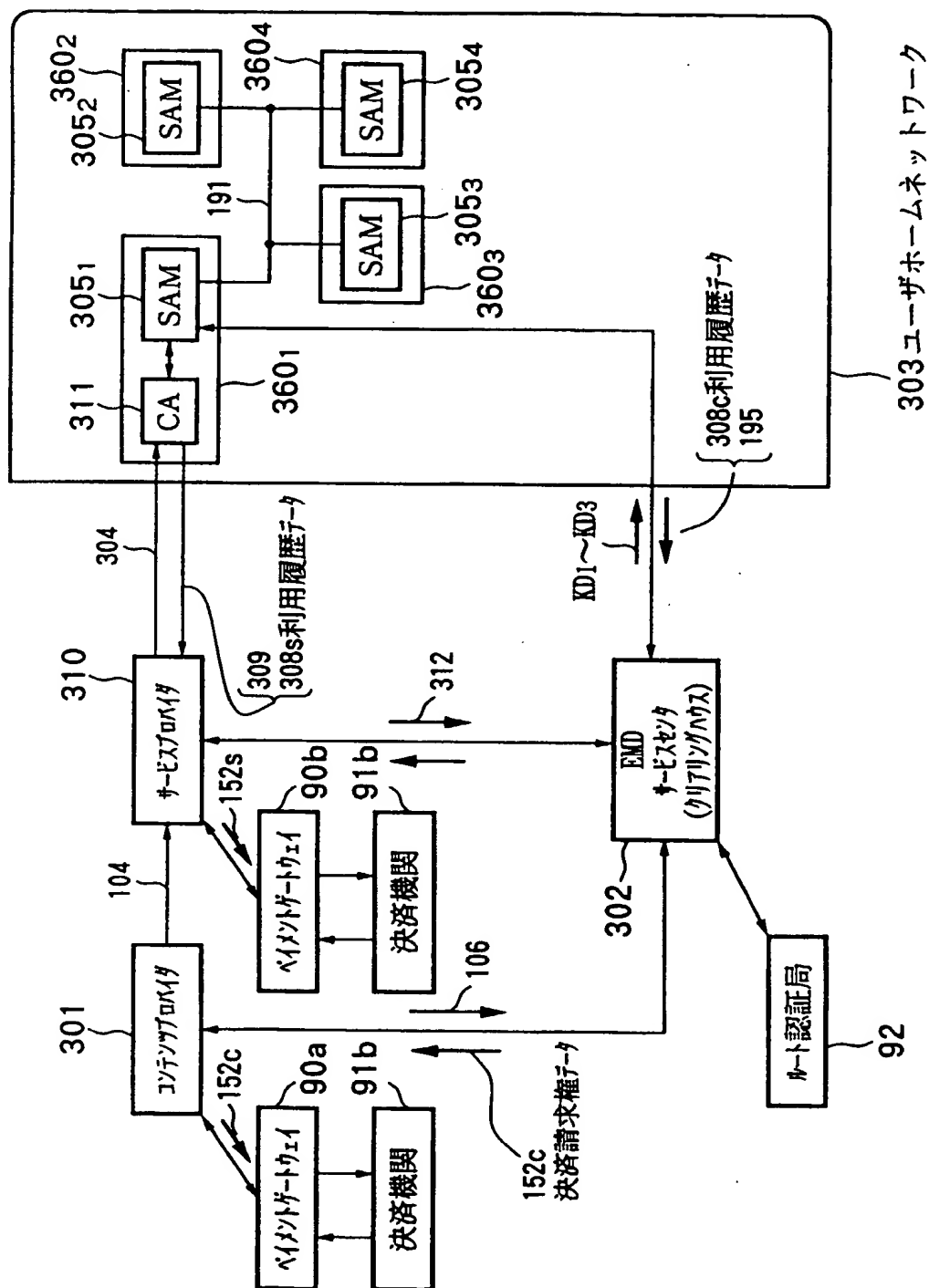
FIG.81



THIS PAGE BLANK (USPTO)

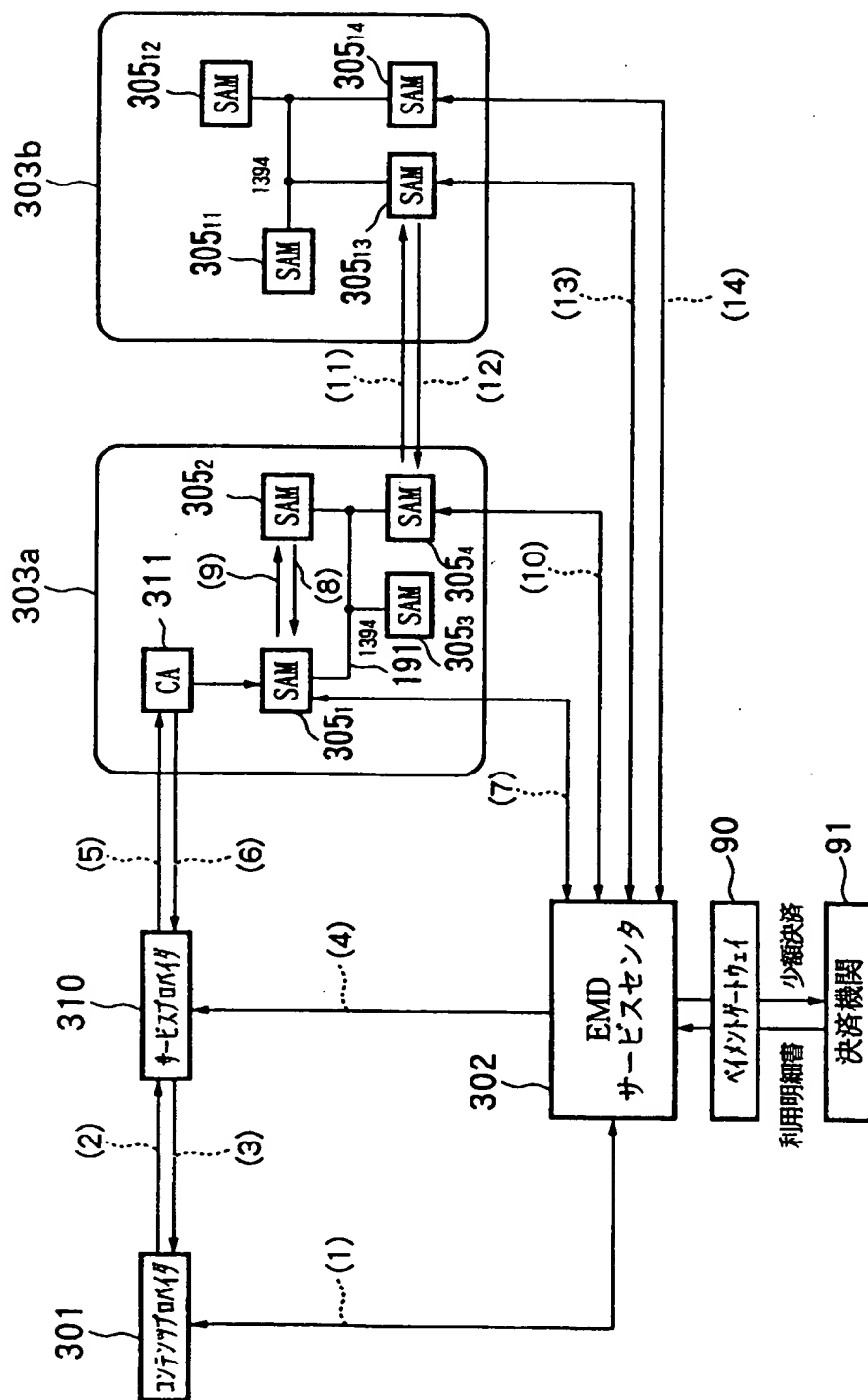
THIS PAGE BLANK (USPTO)

FIG. 83



THIS PAGE BLANK (USPTO)

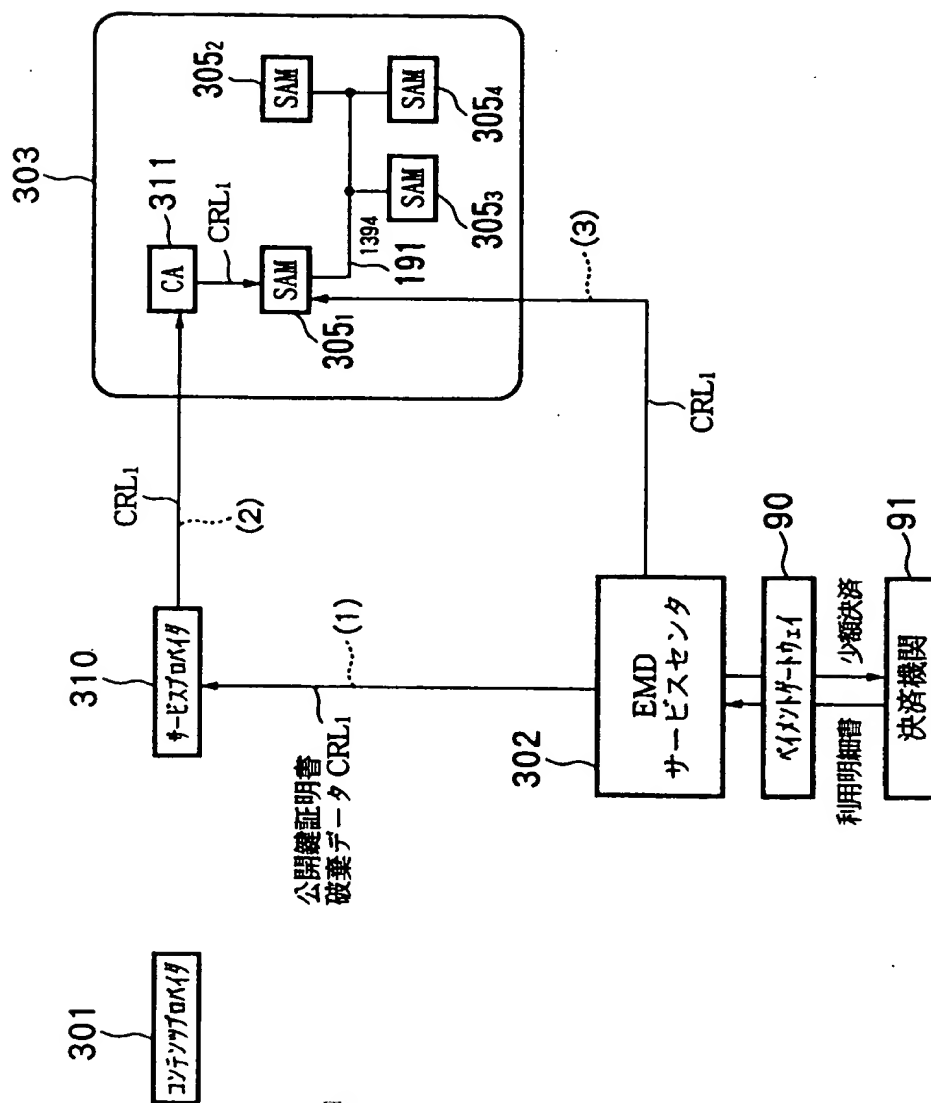
FIG.84



公開鍵証明書の手ルート

THIS PAGE BLANK (USPTO)

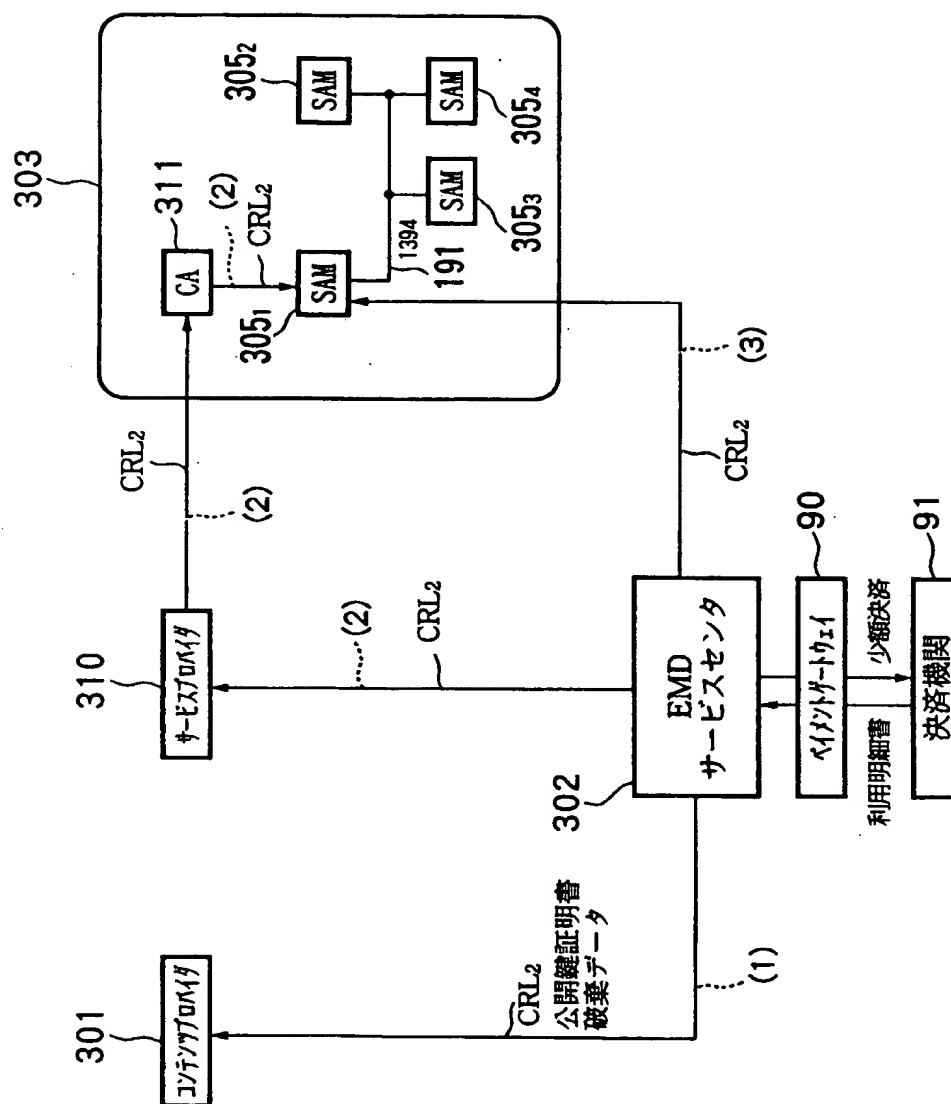
FIG.85



CERCPを無効にする場合

THIS PAGE BLANK (USPTO)

FIG. 86

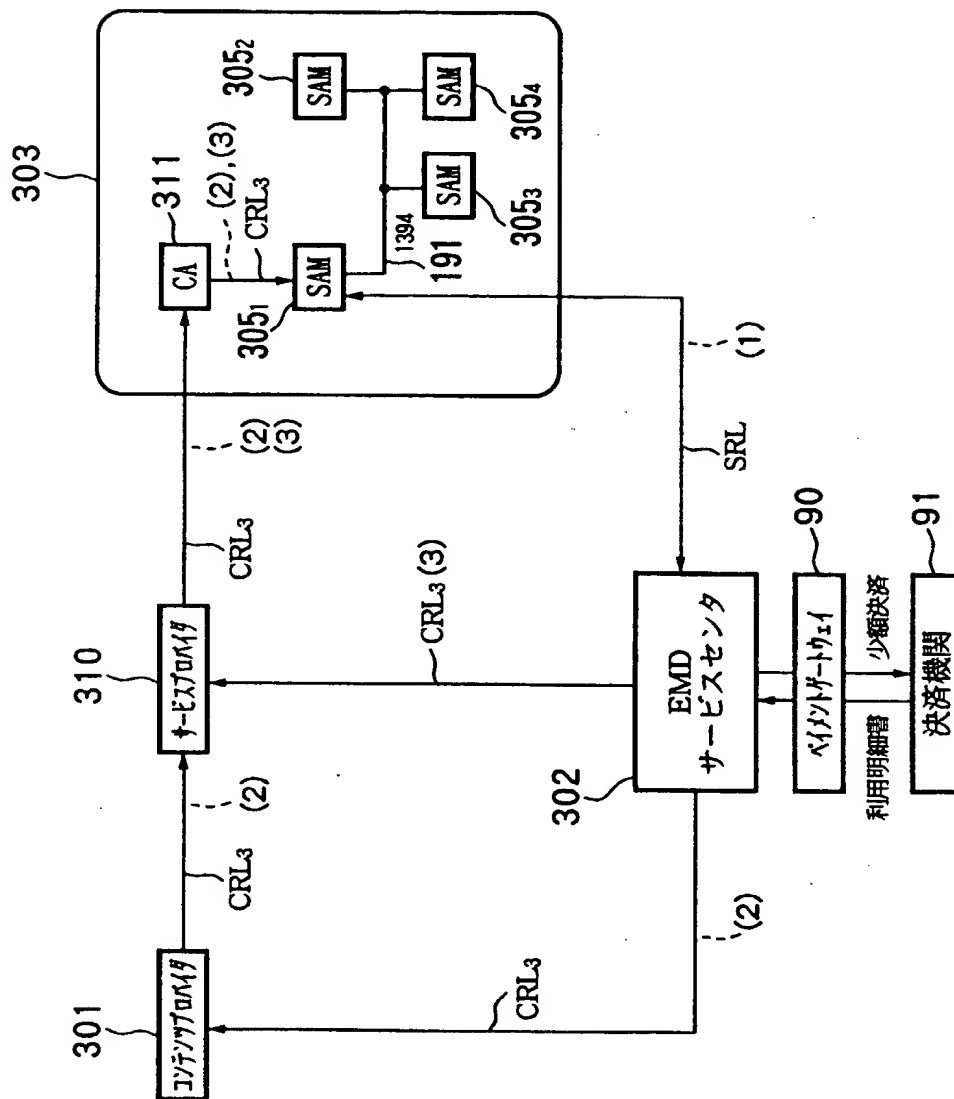


CERSPを無効にする場合

THIS PAGE BLANK (USPTO)

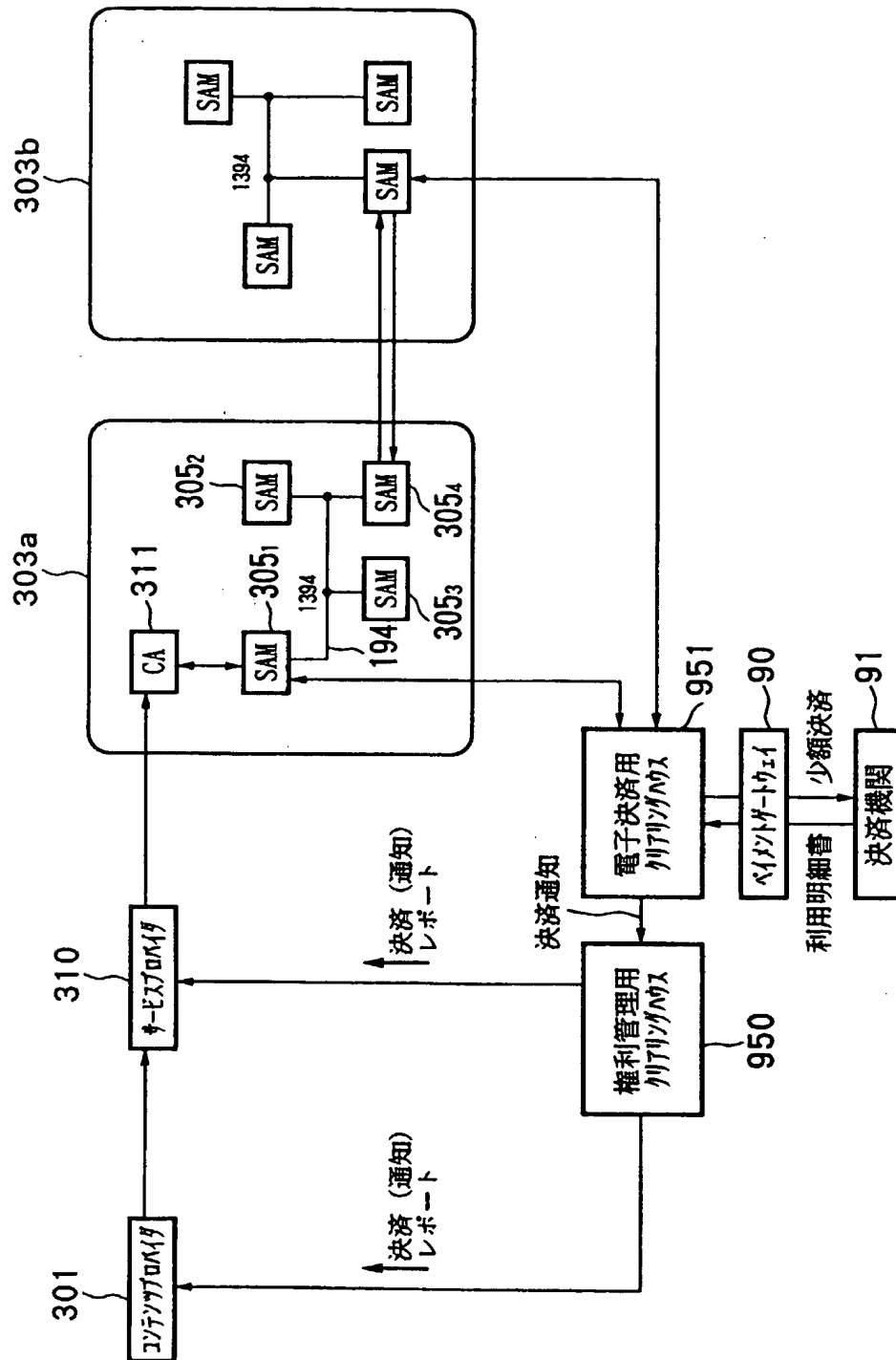
THIS PAGE BLANK (USPTO)

FIG.88



THIS PAGE BLANK (USPTO)

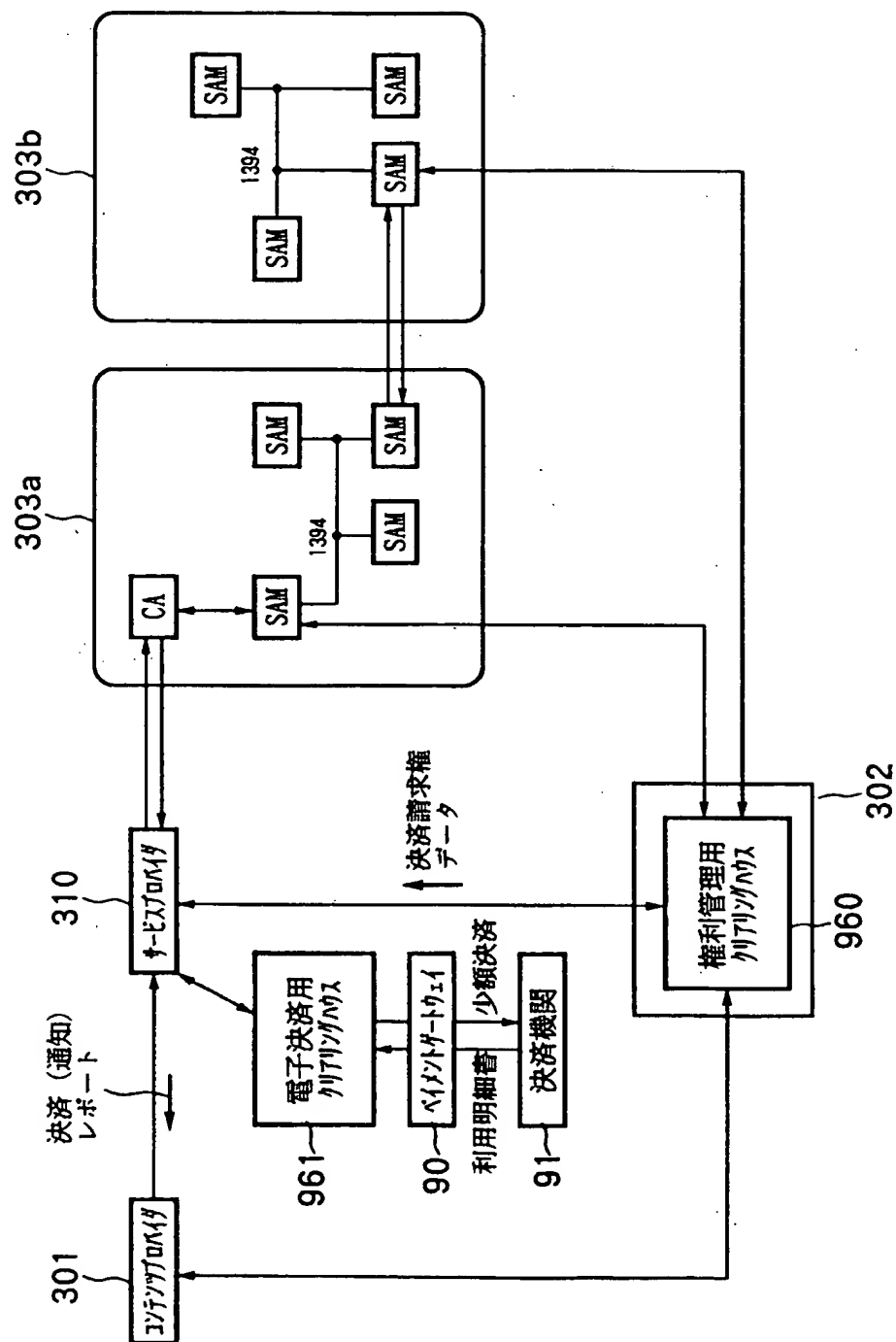
FIG.89



THIS PAGE BLANK (USPTO)

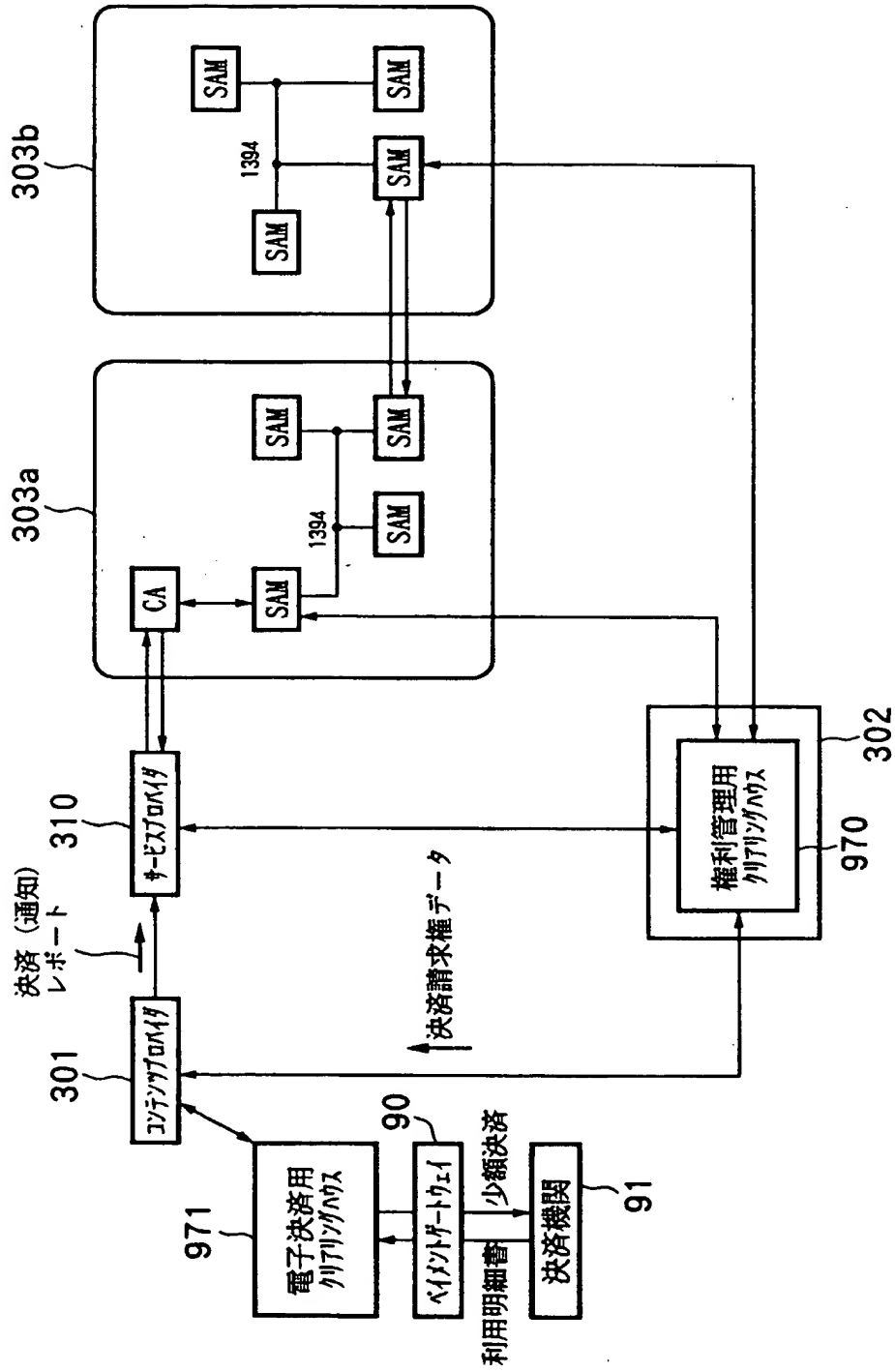
THIS PAGE BLANK (USPTO)

FIG. 91



THIS PAGE BLANK (USPTO)

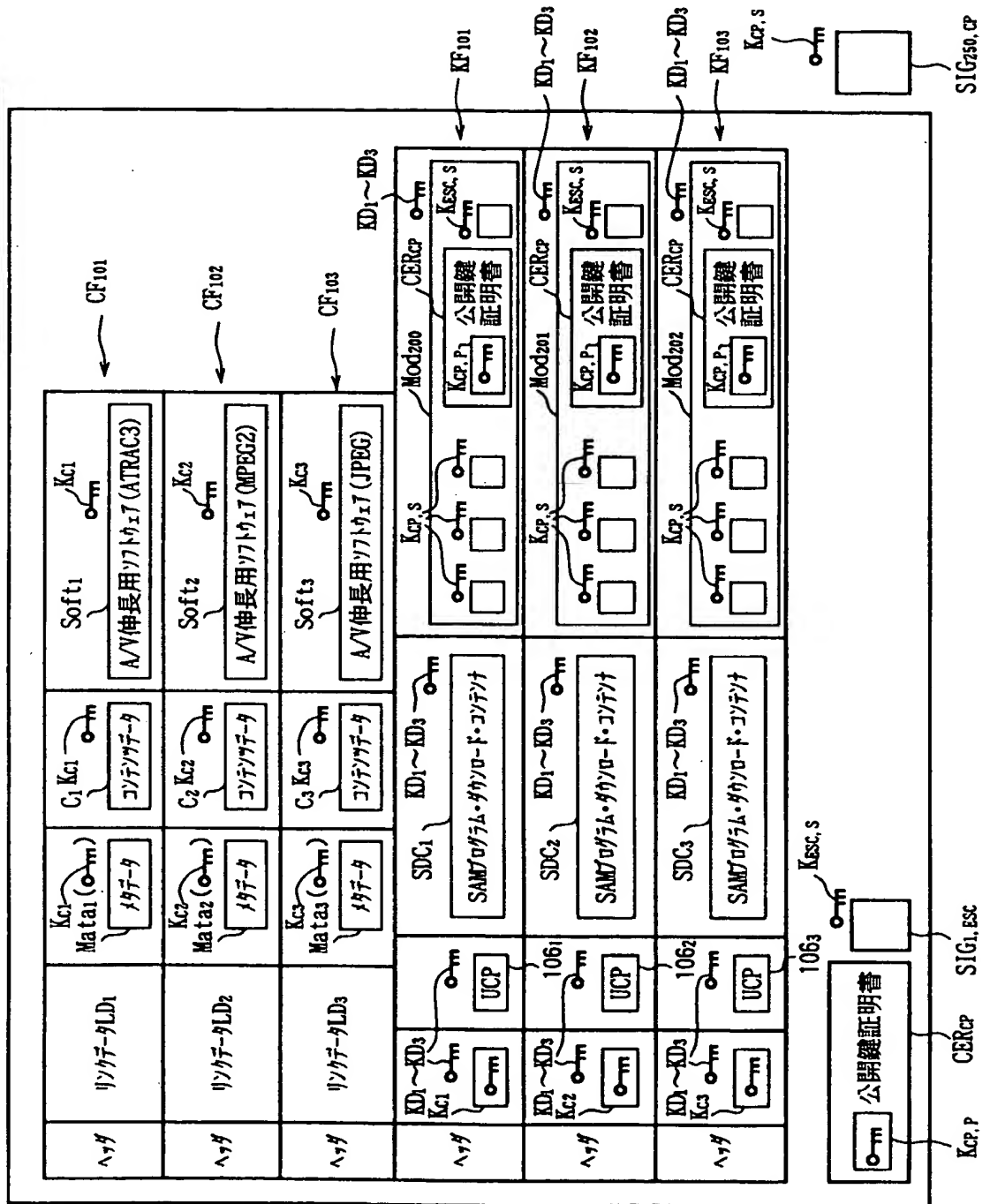
FIG.92



THIS PAGE BLANK (USPTO)

FIG.93

セキユアコンテナ 104a



THIS PAGE BLANK (USPTO)

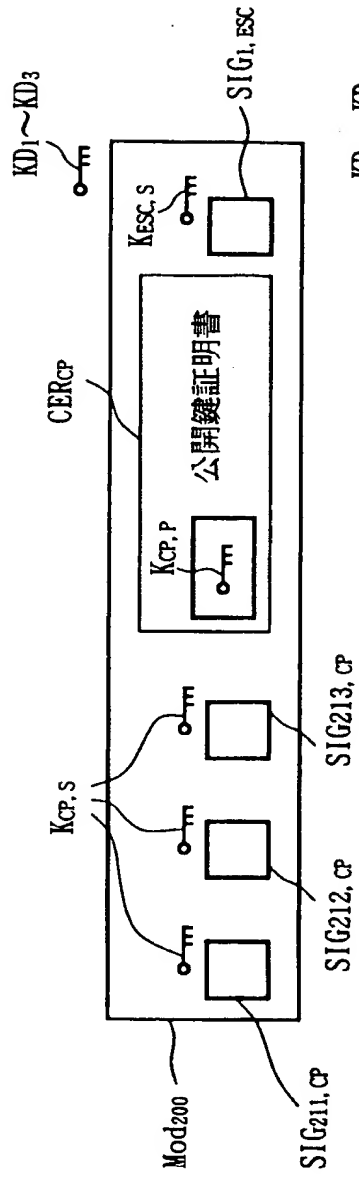


FIG. 94A

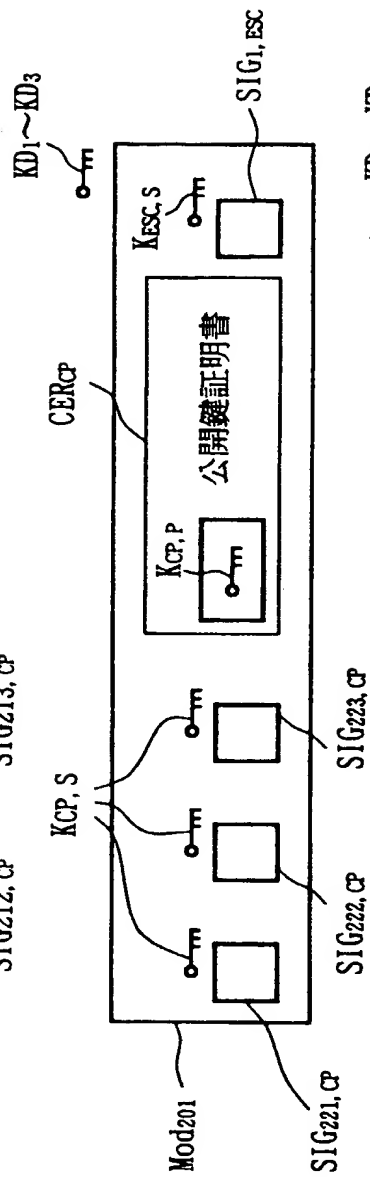


FIG. 94B

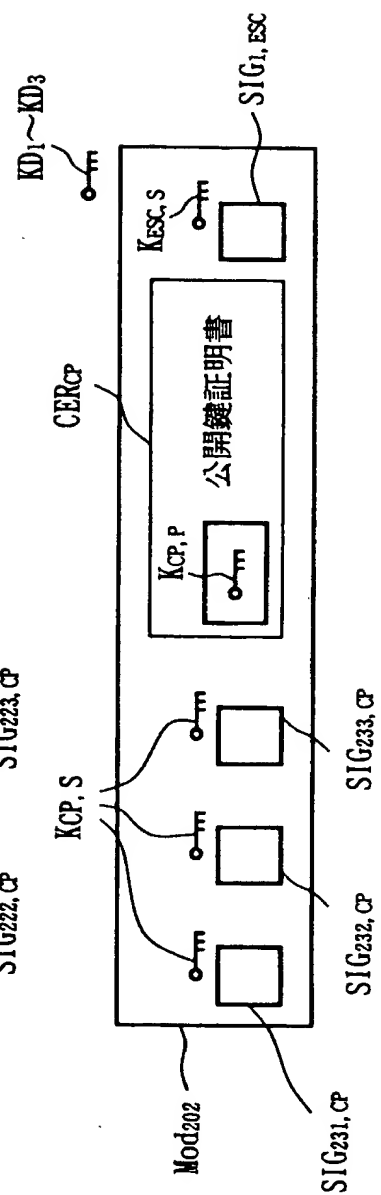
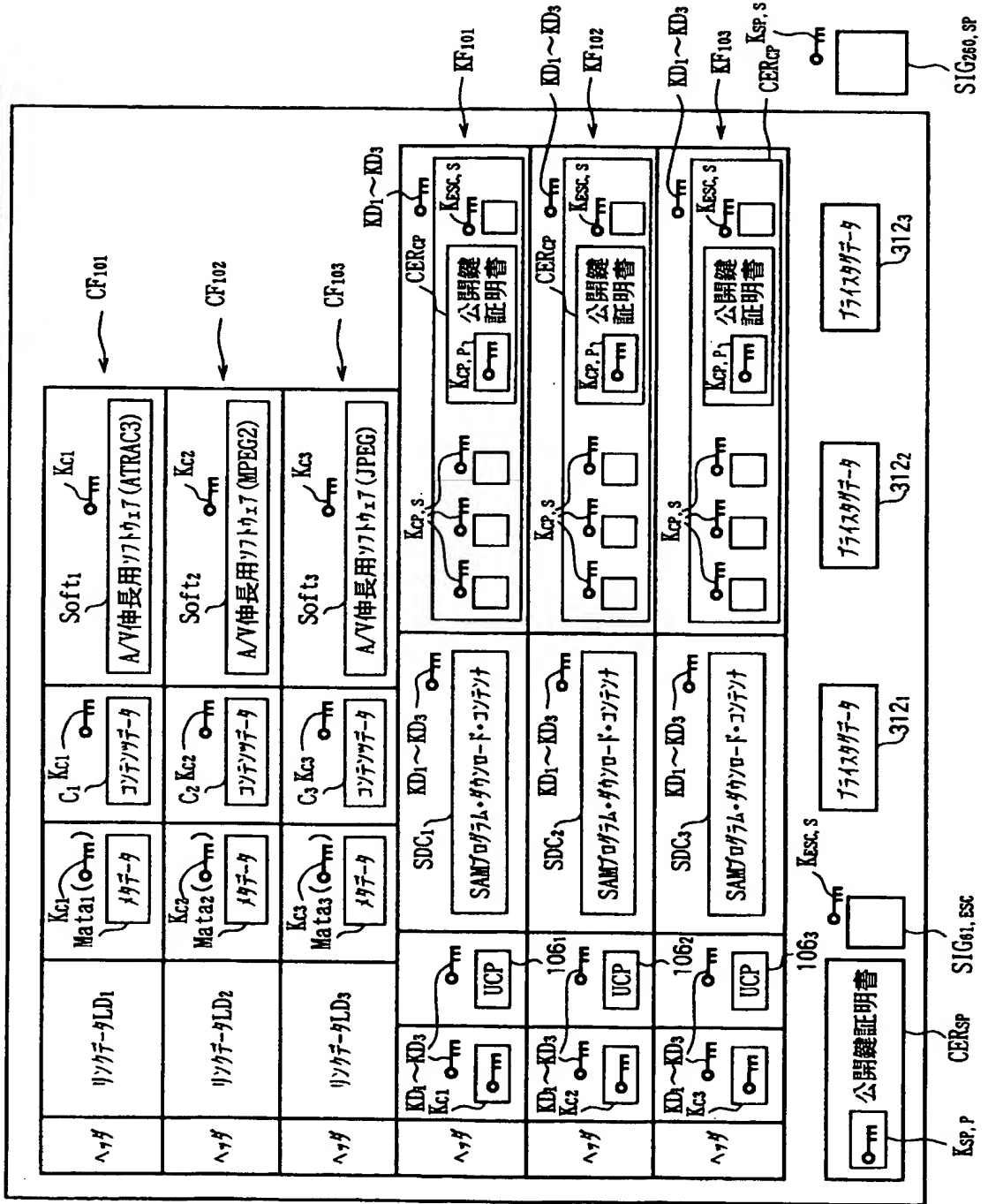


FIG. 94C

THIS PAGE BLANK (USPTO)

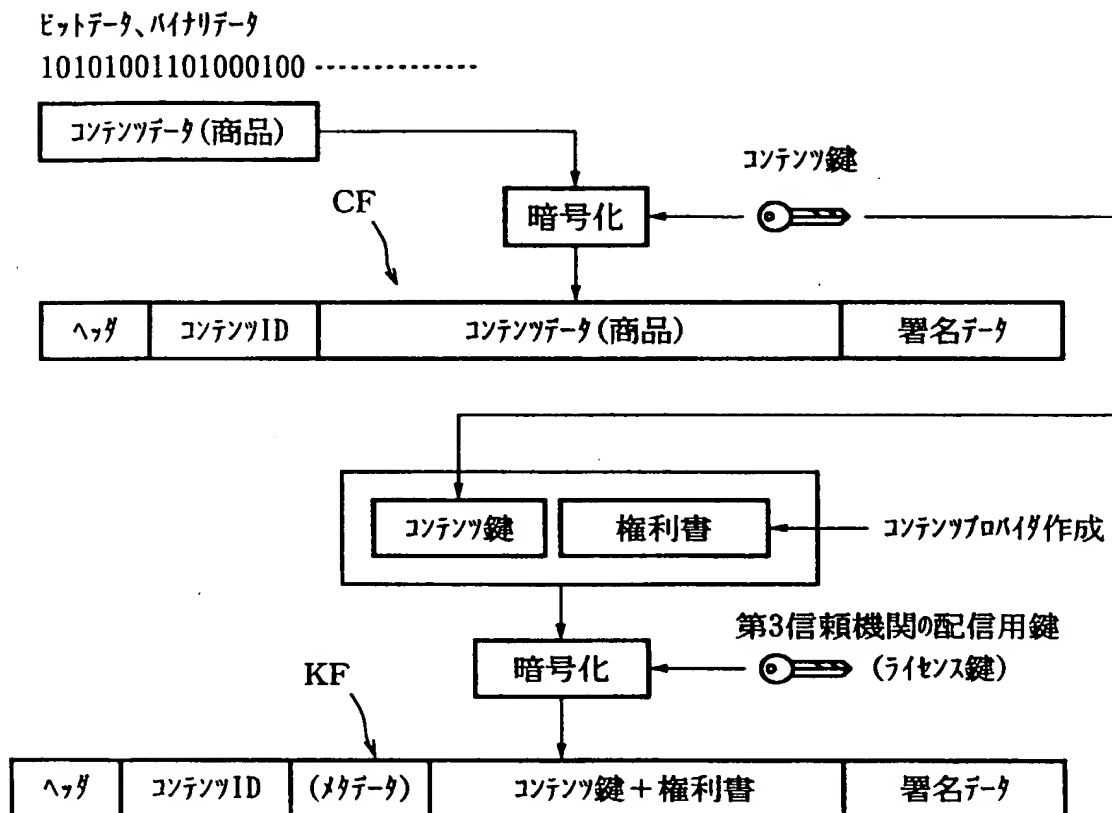
FIG.95

セキュアコンテンツ304a



THIS PAGE BLANK (USPTO)

FIG.96

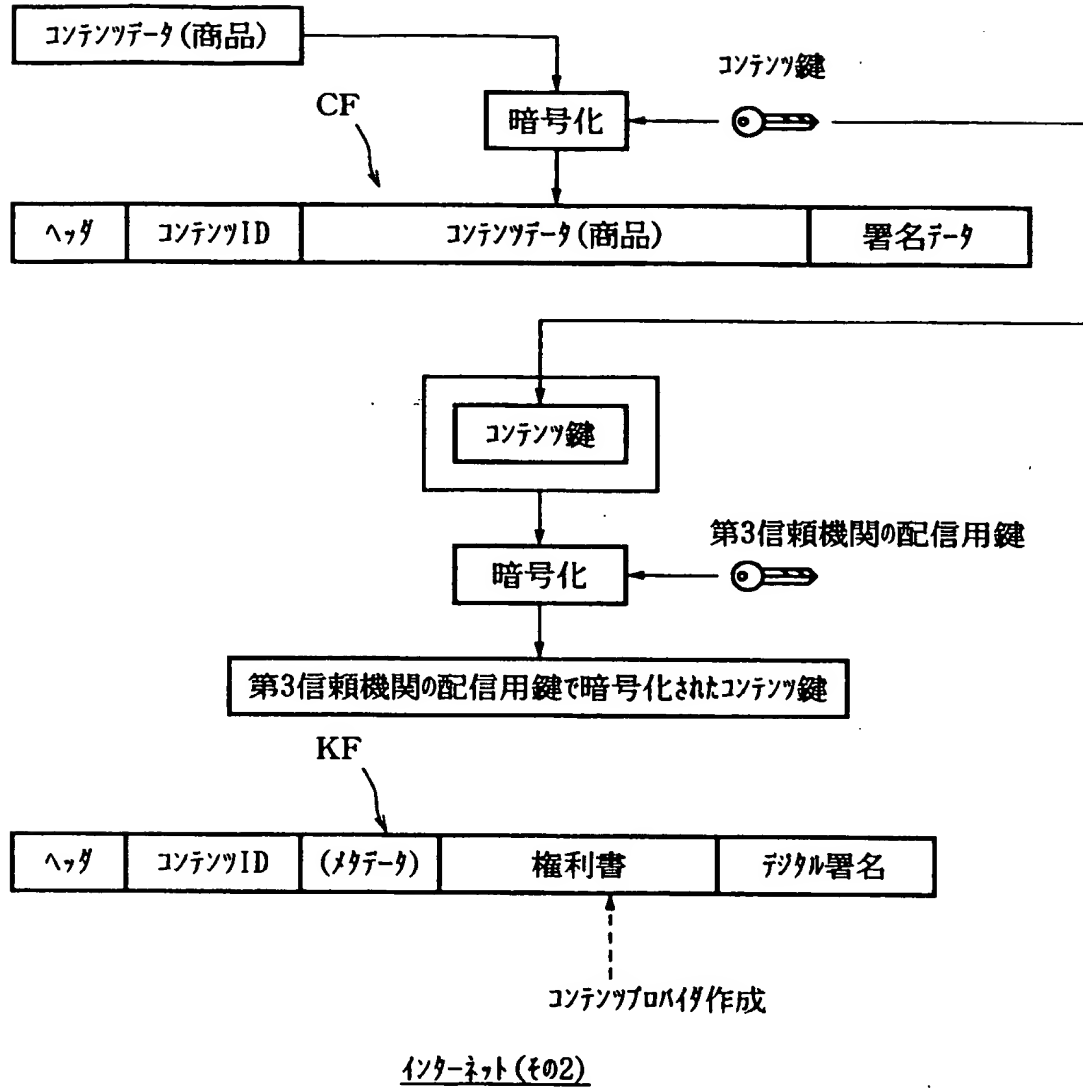
インターネット(その1)

THIS PAGE BLANK (USPTO)

FIG.97

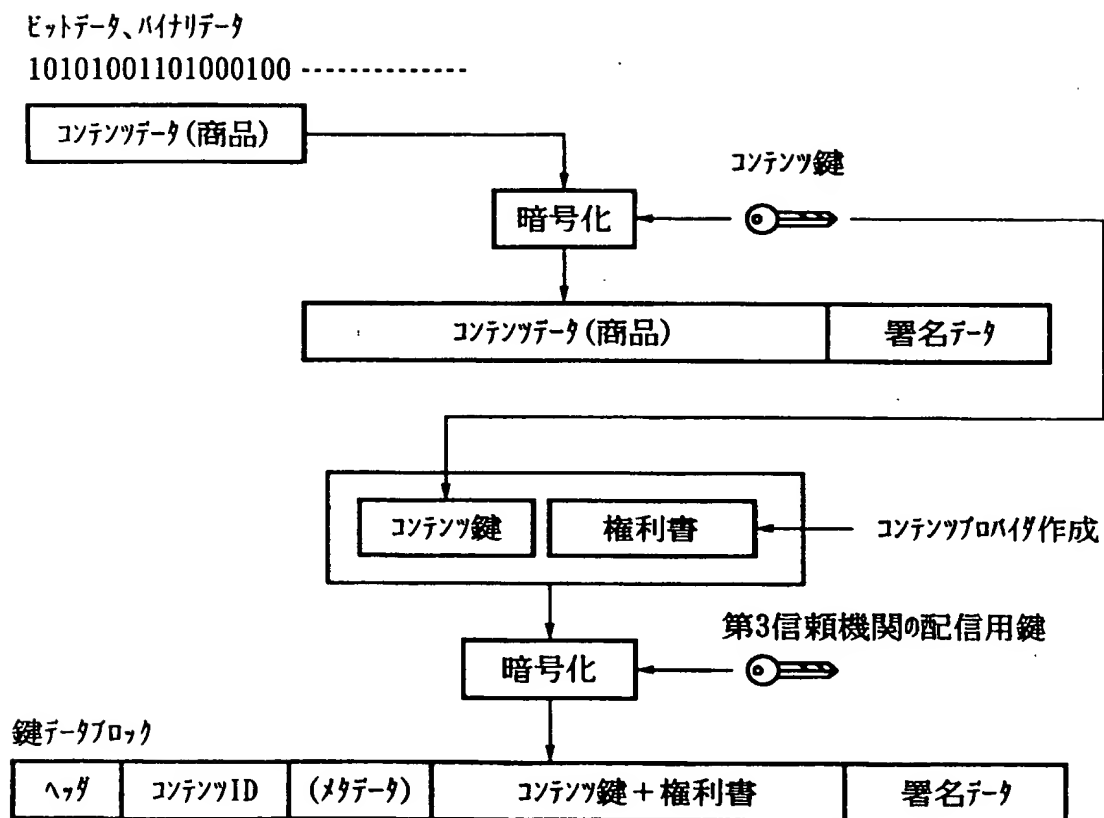
ビットデータ、パリティデータ

10101001101000100



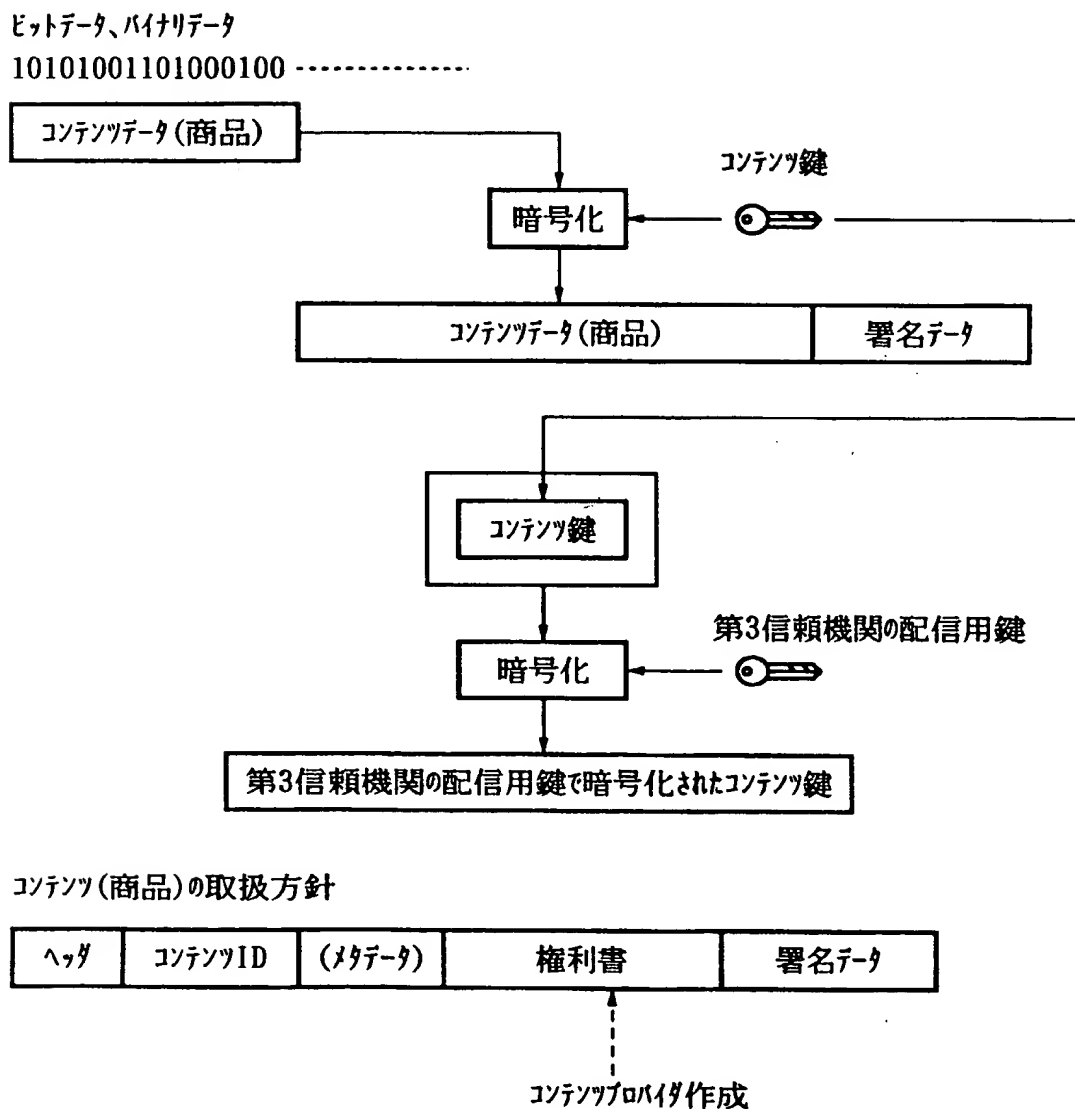
THIS PAGE BLANK (USPTO)

FIG.98

デジタル放送(その1)

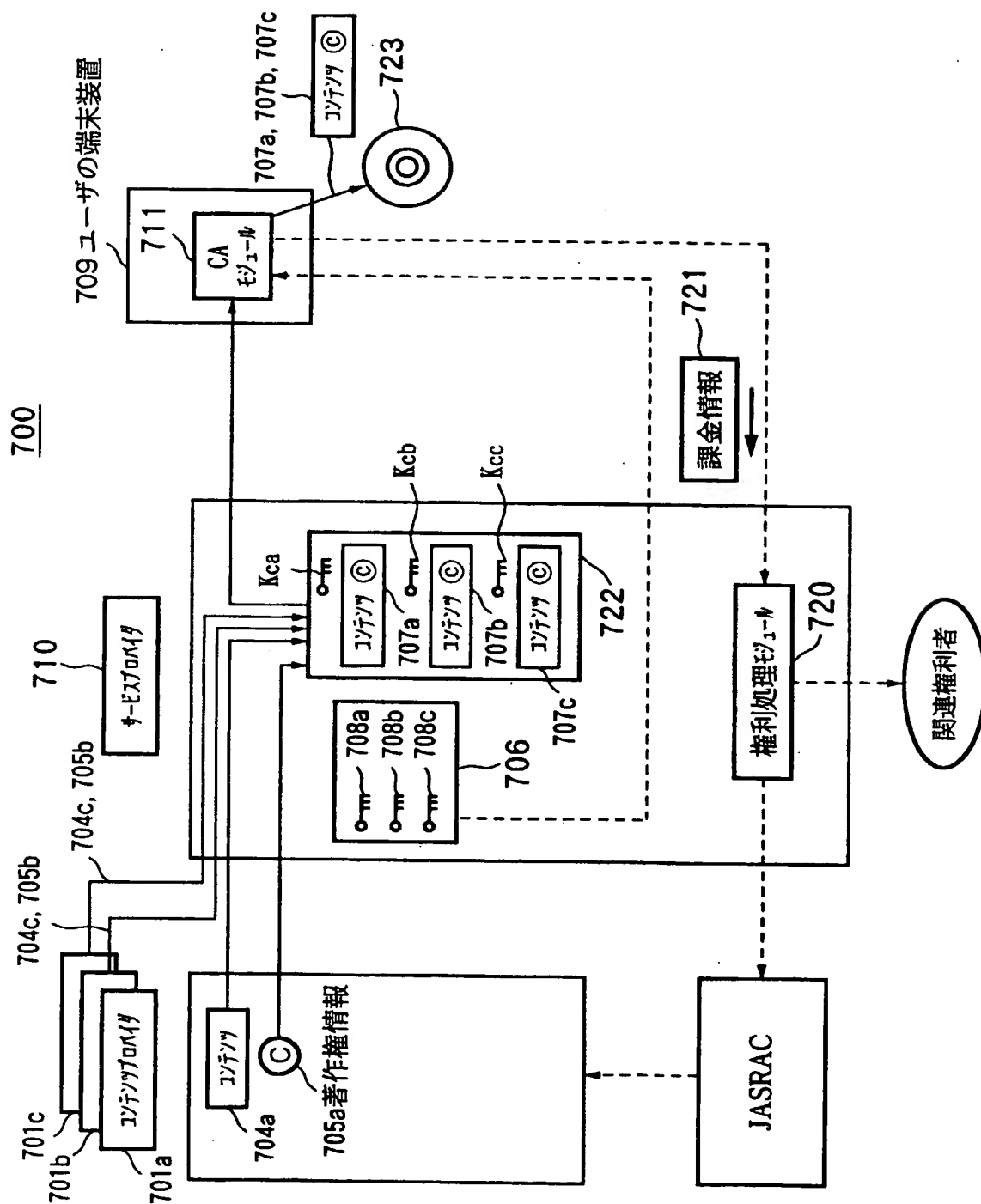
THIS PAGE BLANK (USPTO)

FIG.99

デジタル放送(その2)

THIS PAGE BLANK (USPTO)

FIG.100



THIS PAGE BLANK (USPTO)

符号リスト

90…ペイメントゲートウェイ
91…決済機関
92…ルート認証局
100, 300…EMDシステム
101, 301…コンテンツプロバイダ
102, 302…EMDサービスセンタ
103, 303…ユーザホームネットワーク
104, 304…セキュアコンテナ
105₁ ~ 105₄, 305₁ ~ 305₄…SAM
106…権利書データ
107, 307…決済レポートデータ
108, 308…利用履歴データ
160₁…ネットワーク機器
160₂ ~ 160₄…AV機器
152, 152c, 152s…決済請求権データ
191…バス
310…サービスプロバイダ
311…CAモジュール
312…プライスタグデータ
CF…コンテンツファイル
KF…キーファイル
Kc…コンテンツ鍵データ

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Toroku Jitsuyo Shinan Koho	1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CS DATABASE, WPI, JICST SCIENCE and TECHNOLOGY DOCUMENT DATABASE contents, distribution, SuperDistribution

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), pages 165 to 177, 386 to 412, 597 to 602, 638 to 644 & JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A	1-14, 16-36, 38-71, 142, 150-171, 183-204
Y	& US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	15, 37, 99-108, 110-115, 117-136, 138-141, 175-182, 208
A		72-98, 109, 116, 137, 143-149, 172-174, 205-207
Y	WO, 98/10381, A1 (Intertrust Technologies Corp.), 12 March, 1998 (12.03.98), pages 104 to 142, 168 to 190 (Family: none)	15, 37, 99-108, 110-115, 117-136, 138-141, 175-182, 208

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 November, 2000 (14.11.00)

Date of mailing of the international search report
21 November, 2000 (21.11.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 11-85504, A (Mitsubishi Electric Corporation), 30 March, 1999 (30.03.99), See the full text (Family: none)	1-208
A	JP, 10-161937, A (Toshiba Corporation), 19 June, 1998 (19.06.98), See the full text (Family: none)	1-208

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/04488

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the international application are separated into 14 groups: claims 1-71/ claims 72-76, 79-81, 83-89, 92-95, 97/ claims 77, 78, 82, 90, 91, 96, 98/ claims 99-141, 180-182/ claims 142-149/150, 183/ claims 151, 152, 184, 185/ claims 153, 154, 186, 187/ claims 155-157, 160-165, 188-190, 193-198/ claims 158, 191/ claims 159, 192/ claims 166-171, 199-204/ claims 172-174, 205-207/ and claims 175-179, 208.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

THIS PAGE BLANK (USPTO)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996年
日本国公開実用新案公報	1971-2000年
日本国実用新案登録公報	1996-2000年
日本国登録実用新案公報	1994-2000年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

CSデータベース, WPI, JICST科学技術文献データベース contents, distribution, SuperDistribution

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.) 6.9月.1996(06.09.96), 第165-177, 386-412, 597-602, 638-644頁 & JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	1-14, 16-36, 3 8-71, 142, 150 -171, 183-204
Y		15, 37, 99- 108, 110-115, 117-136, 138- 141, 175-182, 208

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

14.11.00

国際調査報告の発送日

21.11.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

電話番号 03-3581-1101

5M

9364

内線 3599

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		72-98, 109, 116, 137, 143- 149, 172-174, 205-207
Y	WO, 98/10381, A1 (Intertrust Technologies Corp.) 12. 3月. 1998 (12. 03. 98), 第104-142, 168-190頁 (ファミリーなし)	15, 37, 99- 108, 110-115, 117-136, 138- 141, 175-182, 208
A	JP, 11-85504, A (三菱電機株式会社) 30. 3月. 1999 (30. 03. 99), 全頁を参照 (ファミリーなし)	1-208
A	JP, 10-161937, A (株式会社東芝) 19. 6月. 1998 (19. 06. 98), 全頁を参照 (ファミリーなし)	1-208

第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査することを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
。
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるときの国際調査機関は認めた。

この出願の発明は、請求の範囲1-71/72-76, 79-81, 83-89, 92-95, 97/77, 78, 82, 90, 91, 96, 98/99-141, 180-182/142-149/150, 183/151, 152, 184, 185/153, 154, 186, 187/155-157, 160-165, 188-190, 193-198/158, 191/159, 192/166-171, 199-204/172-174, 205-207/175-179, 208の14群の発明に区分される。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

THIS PAGE BLANK (USPTO)

PATENT COOPERATION TREATY

PCT 6491

NOTIFICATION OF RECEIPT OF
RECORD COPY

(PCT Rule 24.2(a))



From the INTERNATIONAL BUREAU

To:

SATOH, Takahisa
Sohshin International Patent Office
4F Miyaki Bldg.
4-2, Yanagibashi 2-chome
Taito-ku, Tokyo 111-0052
JAPON

Date of mailing (day/month/year) 09 August 2000 (09.08.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 00/8046-SNY	International application No. PCT/JP00/04488

The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

SONY CORPORATION (for all designated States except US)

NONAKA, Akira et al (for US)

International filing date	:	06 July 2000 (06.07.00)
Priority date(s) claimed	:	06 July 1999 (06.07.99)
		07 July 1999 (07.07.99)
		07 July 1999 (07.07.99)
		21 April 2000 (21.04.00)

Date of receipt of the record copy by the International Bureau	:	21 July 2000 (21.07.00)
---	---	-------------------------

List of designated Offices

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE
National : CN, KR, US

ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase
☒ confirmation of precautionary designations
☐ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:

Susumu Kube

Telephone No. (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

PATENT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

SATOH, Takahisa
Sohshin International Patent Office
4F Miyaki Bldg.
4-2, Yanagibashi 2-chome
Taito-ku, Tokyo 111-0052
JAPON

Date of mailing (day/month/year) 09 August 2000 (09.08.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 00/8046-SNY	
International application No. PCT/JP00/04488	International filing date (day/month/year) 06 July 2000 (06.07.00)
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 06 July 1999 (06.07.99)
Applicant SONY CORPORATION et al	

- The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
- This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
- An asterisk(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
- The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
06 July 1999 (06.07.99)	11/192413	JP	21 July 2000 (21.07.00)
07 July 1999 (07.07.99)	11/193561	JP	21 July 2000 (21.07.00)
07 July 1999 (07.07.99)	11/193562	JP	21 July 2000 (21.07.00)
21 Apr 2000 (21.04.00)	2000/126305	JP	21 July 2000 (21.07.00)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer

Susumu Kubo

Telephone No. (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

PATENT COOPERATION TREATY

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

SATOH, Takahisa
Sohshin International Patent Office
4F Miyaki Bldg.
4-2, Yanagibashi 2-chome
Taito-ku, Tokyo 111-0052
JAPAN



Date of mailing (day/month/year) 11 January 2001 (11.01.01)		
Applicant's or agent's file reference 00/8046-SNY		IMPORTANT NOTICE
International application No. PCT/JP00/04488	International filing date (day/month/year) 06 July 2000 (06.07.00)	Priority date (day/month/year) 06 July 1999 (06.07.99)
Applicant SONY CORPORATION et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

CN,EP

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 11 January 2001 (11.01.01) under No. WO 01/02968

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

Continuation of Form PCT/IB/308

**NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF
THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES**


Date of mailing (day/month/year) 11 January 2001 (11.01.01)	IMPORTANT NOTICE
Applicant's or agent's file reference 00/8046-SNY	International application No. PCT/JP00/04488
<p>The applicant is hereby notified that, at the time of establishment of this Notice, the time limit under Rule 46.1 for making amendments under Article 19 has not yet expired and the International Bureau had received neither such amendments nor a declaration that the applicant does not wish to make amendments.</p>	

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2000年07月06日 (06. 07. 2000) 木曜日 10時31分20秒

00/8046-

0	受理官庁記入欄		
0-1	国際出願番号		
0-2	国際出願日		
0-3	(受付印)		
0-4	様式-PCT/R0/101 この特許協力条約に基づく国際出願願書は、 0-4-1 右記によって作成された。	PCT-EASY Version 2.90 (updated 10. 05. 2000)	
0-5	0-5 申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。		
0-6	0-6 出願人によって指定された受理官庁	日本国特許庁 (R0/JP)	
0-7	0-7 出願人又は代理人の書類記号	00/8046-SNY	
I	I 発明の名称	データ提供システム、装置およびその方法	
II	II 出願人 II-1 この欄に記載した者は II-2 右の指定国についての出願人である。 II-4ja 名称 II-4en Name II-5ja あて名: II-5en Address: II-6 国籍 (国名) II-7 住所 (国名)	出願人である (applicant only) 米国を除くすべての指定国 (all designated States except US) ソニー株式会社 SONY CORPORATION 141-0001 日本国 東京都 品川区 北品川6丁目7番35号 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国 JP	
III-I	III-I その他の出願人又は発明者 III-I-1 この欄に記載した者は III-I-2 右の指定国についての出願人である。 III-I-4ja 氏名 (姓名) III-I-4en Name (LAST, First) III-I-5ja あて名: III-I-5en Address: III-I-6 国籍 (国名) III-I-7 住所 (国名)	出願人及び発明者である (applicant and inventor) 米国のみ (US only) 野中 聡 NONAKA, Akira 141-0001 日本国 東京都 品川区 北品川6丁目7番35号 ソニー株式会社内 c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan 日本国 JP 日本国 JP	

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2000年07月06日（06.07.2000）木曜日 10時31分20秒

III-2 III-2-1	その他の出願人又は発明者 この欄に記載した者は	出願人及び発明者である (applicant and inventor) 米国のみ (US only)
III-2-2	右の指定国についての出願人である。	江崎 正
III-2-4ja	氏名(姓名)	EZAKI, Tadashi
III-2-4en	Name (LAST, First)	141-0001 日本国
III-2-5ja	あて名:	東京都 品川区 北品川6丁目7番35号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍(国名)	日本国 JP
III-2-7	住所(国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	佐藤 隆久
IV-1-1en	Name (LAST, First)	SATOH, Takahisa
IV-1-2ja	あて名:	111-0052 日本国 東京都 台東区 柳橋2丁目4番2号 宮木ビル4階 創進国際特許事務所
IV-1-2en	Address:	SOHSHIN INTERNATIONAL PATENT OFFICE 4F Miyaki Bldg., 4-2, Yanagibashi 2-chome, Taito-ku, Tokyo 111-0052 Japan
IV-1-3	電話番号	03-3866-4012
IV-1-4	ファクシミリ番号	03-3866-4022
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE 及びヨーロッパ特許条約と特許協力条約の締約国 である他の国
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	CN KR US
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2000年07月06日（06. 07. 2000）木曜日 10時31分20秒

V-6	指定の確認から除かれる国	なし (NONE)	
VI-1	先の国内出願に基づく優先権主張	1999年07月06日 (06. 07. 1999) 特願平11-192413 日本国 JP	
VI-1-1	先の出願日		
VI-1-2	先の出願番号		
VI-1-3	国名		
VI-2	先の国内出願に基づく優先権主張	1999年07月07日 (07. 07. 1999) 特願平11-193561 日本国 JP	
VI-2-1	先の出願日		
VI-2-2	先の出願番号		
VI-2-3	国名		
VI-3	先の国内出願に基づく優先権主張	1999年07月07日 (07. 07. 1999) 特願平11-193562 日本国 JP	
VI-3-1	先の出願日		
VI-3-2	先の出願番号		
VI-3-3	国名		
VI-4	先の国内出願に基づく優先権主張	2000年04月21日 (21. 04. 2000) 特願2000-126305 日本国 JP	
VI-4-1	先の出願日		
VI-4-2	先の出願番号		
VI-4-3	国名		
VII-1	特定された国際調査機関 (ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	4	-
VIII-2	明細書	170	-
VIII-3	請求の範囲	68	-
VIII-4	要約	1	00804601. txt
VIII-5	図面	99	-
VIII-7	合計	342	
VIII-8	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1, VI-2, VI-3, VI-4	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-17	その他	国際事務局の口座への振込を証明する書面	-
VIII-18	要約書とともに提示する図の番号	1	
VII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印	<div style="display: inline-block; border: 1px solid black; padding: 2px;">久佐介 の 印</div>	
IX-1-1	氏名 (姓名)	佐藤 隆久	

受理官庁記入欄

T0-1	国際出願として提出された書類の実際の受理の日	
------	------------------------	--

THIS PAGE BLANK (USPTO)

特許協力条約に基づく国際出願願書

原本（出願用） - 印刷日時 2000年07月06日（06.07.2000）木曜日 10時31分20秒

10-2	図面：	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類を補完する書類又は図面であつてその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第II条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	
------	-----------	--

THIS PAGE BLANK (USPTO)

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. It is the applicant's responsibility to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

THIS PAGE BLANK (USPTO)